National Telecommunications and Information Administration
Department of Commerce
1401 Constitution Avenue, NW
HCHB Room 7324
Attn.: FirstNet NOI
Washington, DC 20230

Comments from: Law Enforcement and Intelligence Consulting, LLC
Mark Tanner, President

The need for better public safety communications is not a new problem. It predates 9/11. We have been following the D-Block and public safety communications for a number of years. According to the 9/11 Commission recommendations, "Congress should support pending legislation that provides for the expedited and increased assignment of radio spectrum for public safety purposes." Since 9/11, there have been a number of organizations working to improve public safety communications. The passing of the Middle Tax Relief and Job Creation Act of 2012, which provides allocation of the D-Block to public safety and the formation of the First Responder Network Authority (FirstNet), presents tremendous opportunities and challenges. The National Telecommunications and Information Administration (NTIA) is to be commended on the selection of a diverse and experienced FirstNet Board. From the first FirstNet Board meeting, it is obvious that the Board members are committed to finding a solution to the public safety communications challenges.

The FirstNet Board faces complex issues in managing the deployment and operation of the FirstNet Nationwide Network (FNN). While technical and logistical challenges have been address by the mobile network operators and system integrators, the requirements of public safety, present new and unique challenges. The public safety community is diverse in geography, capability, and mission. Several public safety groups, including the National Public Safety Telecommunications Council (NPSTC), SAFECOM, and others have made great strides in defining public safety communications requirements. However, constant, continuous communications is going to be necessary to address this diverse group of customers. Finally, the business plan for funding of FNN must be reasonable for state, local, and tribal first responders to participate. If not, they may opt-out, as allowed under the law, or otherwise stymie the deployment.

The presentation of FirstNet Board member Craig Farrill provides a vision for the future. Making use of commercial infrastructure, as implemented by mobile network operators, presents opportunities to leverage costs/investments and adopt proven interoperability standards. However, unique requirements of public safety are not addressed by commercial mobile networks today. The following observations are offered concerning the notice of inquiry:

1. Meets public safety's requirements for priority, quality of service, and preemption features.

The presentation (slide 8) identifies a "pro" for the creation of a diverse nationwide network with multiple networks and systems as "higher reliability." I would rather characterize the pro as "higher availability" by taking advantage of the already deployed mobile networks. The commercial networks, as they are deployed today, provide superior coverage and are therefore, highly available. However, they do not meet public safety requirements for reliability. For instance, they do not provide all of the features of mission critical voice as defined by the NPSTC:

- **Direct or Talk Around:** This mode of communications provides public safety with the ability to communicate unit-to-unit when out of range of a wireless network OR when working in a confined area where direct unit-to-unit communications is required.

- **Push-to-Talk (PTT):** This is the standard form of public safety voice communications today - the speaker pushes a button on the radio and transmits the voice message to other units. When they are done speaking they release the Push-to-Talk switch and return to the listen mode of operation.

- **Full Duplex Voice Systems:** This form of voice communications mimics that in use today on cellular or commercial wireless networks where the networks are interconnected to the Public Switched Telephone Network (PSTN).

- **Group Call:** This method of voice communications provides communications from one-to-many members of a group and is of vital importance to the public safety community.

- **Talker Identification:** This provides the ability for a user to identify who is speaking at any given time and could be equated to caller ID available on most commercial cellular systems today.

- **Emergency Alerting:** This indicates that a user has encountered a life-threatening condition and requires access to the system immediately and is, therefore, given the highest level or priority.

- **Audio Quality:** This is a vital ingredient for mission critical voice. The listener MUST be able to understand without repetition, and can identify the speaker, can detect stress in a speaker's voice, and be able to hear background sounds as well without interfering with the prime voice communications.

Today, many of the capabilities in land mobile radio (LMR) systems (i.e., quality of service, low latency, floor control, etc.) may not be available in LTE systems. Industry should be challenged to meet as many as possible, as soon as practical. The reliability of these LMR systems is superior to commercial systems, as they are designed for the volume of public safety users they support. Commercial systems are widely available, but not reliable in a crisis situation. Preemption on commercial networks is an option to meet with reliability standards for public safety. However, preemption decisions present some interesting questions:

- Who has the authority to initiate a preemption?
- What are the criteria and/or circumstances that warrant preemption?
- What is the liability for preempting a non-public safety user in time of crisis (e.g., heart attack)?

2. Uses, to the extent possible, existing radio access network and core network infrastructure installed by commercial mobile operators in order to maximize the coverage and performance delivered to public safety while minimizing the capital expenditures.

The presentation proposes maximum use of this infrastructure, by having fail-over access to a terrestrial mobile network when FNN is not available and mobile satellite network when that is not available. Consideration could be given to leveraging existing terrestrial mobile networks infrastructure without the reliance on the network itself. For instance, install radio equipment for the public safety band within existing infrastructure and add antennas to existing towers. Existing coverage maps are proven, but would need to be evaluated for this spectrum. Additional work would remain to determine the data capacity requirements of public safety.

Commercial networks likely have capacity for day-to-day operations. Where they are used, accommodations must be made for crisis operations. Having deployable infrastructure for planned events and crises may be an interim solution. Having some deployable infrastructure will be a diminishing continuing need as the FNN extends coverage. At the end-state, a deployable infrastructure should only be needed when permanent sites are destroyed or an area's coverage was never planned.

3. Reaches operational capability as quickly as possible.

The proposed design would meet this objective if features of the design (i.e., fail-over to commercial networks) can be met. The challenges in implementing this design include:

- Devices need to be designed and manufactured to allow for automatic connections to the available network (FNN, Terrestrial Mobile 1, 2, …, Mobile Satellite).
- Multiple chip-sets in such devices will present power and size challenges.
- With limited numbers of public safety users for such devices, they may prove too costly.
- Subscription costs for the possibility of connecting to multiple mobile networks may be prohibitive.

4. Enables voice services (cellular telephony and push-to-talk (PTT) both within the First Net network as well as to/from other commercial networks, including the public switched telephone network (PSTN).

PTT is mentioned within the presentation as part of the service delivery platform. However, no specifics are discussed. Such capability is currently available from several companies. In my view, the one with the most robust features and usability is available from SLA Corporation. See: www.sla-ptt.com

Enterprise Secure Chat (ESChat) is a Real Time PTT system that is carrier independent, and features cross carrier communications. Additionally, LMR interoperability has been configured. ESChat includes a rich feature set supporting the needs of a public safety work force, including AES-256 Voice Encryption that meets the NSA Suite 'B' Standards for protection of Top Secret information.

Framework for Developing Applications

1. Suggestions for applications that would benefit public safety users:

- National Crime Information Center (NCIC) and the FBI's Next Generation Identification (NGI)
    - ability to identify wanted and missing persons
    - stolen property
    - fingerprint capture/checks
    - facial recognition
- Agency records database access – the ability to query names and view documents from mobile devices.
- Geospatial applications for mapping of crime data.
- Blue and Red Force tracking.
- Real-time video from stationary video cameras.
- eGuardian/Suspicious Activity Reporting System (SARS)
- Operational Response and Investigative Online Network (ORION) via FBI Law Enforcement Online (LEO)
- Other LEO, Homeland Security Information Network (HISN), and Regional Information Sharing Systems (RISS) applications

2. Interface requirements and other information innovators need in order to develop applications in an open environment:

Not available

3. Specific security requirements public safety needs in its applications:

- Advanced Encryption Standards (AES), 256 bit encryption for data in transit.
- Two-factor authentication to access information on public safety mobile devices.
- Ability to remotely wipe a mobile device if lost or stolen.
- Federated identity management
- Some of the above can also be addressed not as specific applications, but can be built into the structure of the network itself. For example, the military is expanding the use of so-called zero clients, in which a stateless device is the end user device. This device has only the operating system (OS) necessary to ping the network, and transmit a user's authentication information. Once this is accomplished, the OS is actually replaced on the device by one provisioned from the core, which has been personalized for that specific user. The user then has full access to network resources. The device has no memory of its own, so when the device is turned off all

information is lost. It can also be re-provisioned from the core with a blank OS, effectively wiping it in the event of loss or theft.

- Security is also dramatically enhanced, as only applications and data that are provisioned are resident on the device. Having an on board encoder or USB access would be possible at the discretion of the using agency, but access to the encoder or input device would be controlled by security policies enforceable from the core.
- Because applications are provisioned from the core and are not resident on the end user device, the "app store" concept becomes obsolete. There is no need, for example, to "push" updates to end users, as all provisioned applications come from the same resident file: updating that file updates all files that are provisioned from that file. This cloud based view may hold significant benefits to the PSBN, both in terms of performance and latency, but also in terms of cost. For example, a zero client bend user device would not need memory, a power consumer and physical cost to the end user device.

4. Ideas as to what framework or organizational factors would allow for the development of the greatest number of quality applications:

Establish a public safety innovation collaboration center, under SAFECOM to promote industry development, showcase, and sharing of innovations. The center would benefit from having a research and development lab where products could be integrated and tested for use on the network.

5. Suggestions for FirstNet's applications certification requirements:

- Security certification and accreditation (C&A)
- Testing for mobile development challenges including memory and processor limitations, intermittent network access, and limited battery power
- Mobile applications are first tested within the development environment using emulators and later subjected to field testing

6. Possible delivery methods (e.g. app store models):

- Agency specific applications would be approved for use and loaded per the respective agency governance and technology.
- Nationally available applications would be made available on an app store maintained on either the Homeland Security Information Network (HSIN) or Law Enforcement Online (LEO). The identity of an authorized user would be verified by the federated identity management.

7. Other

Whereas public safety communications systems to date have been mostly concerned with coverage, the FNN must be equally concerned with capacity. It may be necessary to disable some applications in a crisis if they are considered to be data-hogs and/or not mission critical. Since the network capacity will be designed for crisis management, day-to-day use should realize excess capacity. However, during a crisis, and depending on the scope, capacity may be limited.

Business Plans

No specific questions were asked about the business plans and none were identified in the presentation. The business plan for funding the network is going to be a critical component for its acceptance. Most public safety organizations have limited budgets and cannot afford high subscription fees or high-priced devices. FirstNet should seek to identify sources of revenue to defray costs to public safety users. Possibilities include:

- Lease excess capacity during non-crisis times to other users. Other users may include those that rely on public safety, but are not consider part of public safety. For instance, the following critical infrastructure providers:
    - Transportation
    - Energy
    - Food and agriculture
    - Postal and shipping
    - Water
- Applications developed by one agency could be sold to another.

Conclusion

FirstNet is faced with the deployment of a complex system. Industry has experience in the deployment of LMR and LTE systems, but has not had to meet the unique requirements of public safety for broadband wireless services. This is a diverse user community, with unique and diverse requirements.

I applaud the FirstNet Board for their commitment and vision to push the envelope of technology. The design described during the FirstNet Board meeting presents many challenges. Similarly, some of the requirements are not currently met with products currently manufactured. The wireless industry can meet those challenges with the proper incentives, business plans, and leadership of the FirstNet Board.

To meet the challenges, it is critical for the FirstNet Board to have a trusted industry partner serving as the "honest broker." This industry partner (Program Manager, rather than system integrator) must be fully accountable to FirstNet, and should hold companies that provide services and products accountable to deliver on public safety requirements. The Program Manager must provide cost-control for the program by following industry-standard program management practices. They must also be responsible for collecting, synthesizing, and managing requirements from the diverse customer community, interfacing with agencies and organizations in support of the FirstNet Board. Similarly, they must assist the FirstNet board with the acquisitions process to provide transparency and remove any conflict of interest concerns that would slow the program down. The FirstNet Board members are not employed on a full-time basis and their full-time staff will need this expertise to deliver a quality product to the public safety community. The Program Manager should be experienced in managing suppliers and system integrators to deliver the solution for FirstNet and public safety, and they should be brought on via competitive RFP as soon as possible.

About Law Enforcement and Intelligence Consulting, LLC

Law Enforcement and Intelligence Consulting, LLC was founded by Mark Tanner in 2011. He is senior executive with a wide range of experience in law enforcement, intelligence, and business. Following a 23 year career with the Federal Bureau of Investigation (FBI), he has held director and executive level positions in small, medium, and large companies. Mr. Tanner and his colleagues provide innovation and leadership to improve the mission of law enforcement and intelligence agencies. Client companies are able to grow business, making use of their skills in establishing long-term relationships, problem solving, and organizing for success.

Contact:
Mark Tanner
LawEnforcement.Intel@gmail.com
443-223-5055