Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

MAY 31, 2012

In the matter of:	)
	)
Public Safety and Homeland Security Bureau	)
Makes Available the Recommendations of the	)
Technical Advisory Board for First Responder	)
Interoperability	)

To: The Commission; FCC Technical Advisory Board for First Responder Interoperability

COMMENTS OF THE STATE OF MINNESOTA

The following comments are in response to the Commission's publication of the Recommend Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network (NPSBN), dated May 22, 2012.

The hard work of the Commission's Technical Advisory Board for First Responder Interoperability ("Advisory Board") should not go without notice. The subject matter experts appointed to the Advisory Board have made good progress on meeting their statutory duty, successfully publishing a comprehensive set of requirements within a very short timeline, as volunteers, and in addition to their everyday work. Minnesota, and the public safety community as a whole, should recognize their great contribution.

The state of Minnesota hereby offers the following comments for consideration by the Commission, the Advisory Board, and Firstnet:

1. In general, the NPSBN MUST provide neutral transport to the greatest extent possible.

A number of the Advisory Board's recommendations would require that the NPSBN provide relatively neutral transport for local public safety users in order to allow, for example, mobile devices and locally-hosted applications to function on the NPSBN as they do today on private or commercial networks. Accordingly, the NPSBN MUST provide neutral transport where possible subject to reasonable network management.

2. Firstnet should establish a "supported" run-time environment for NPSBN mobile devices.

Interoperability efforts would be enhanced by establishing a "supported" run-time environment for mobile devices on the NPSBN, such as a specific operating system and version of that operating system. A supported

run-time environment would enhance interoperability by greatly simplifying the interactions that must occur to exchange multimedia between two separate mobile devices utilizing the NPSBN. It would streamline testing and acceptance processes as well as applications versioning.

Additionally, a single supported run-time environment would provide a significantly more competitive applications marketplace, as the economy of scale for any public safety application would be the entire public safety community. To have a number of competing run-time environments based on certain providers or equipment manufacturers would, presumably, tie applications horizontally with the device—intentionally or not.

3. Per Recommendations 1.4.1 (3), (7), and (8), the network MUST support locally or regionally deployed applications.

The Advisory Board recommends that existing public safety applications, field-deployed server applications, et al. *should* be supported by the NPSBN. To the contrary, the NPSBN MUST support locally-hosted applications. There already exist today numerous public safety applications, such as CAD and AVL, running over commercial or private wireless data networks, including cellular networks. These applications are not only essential to the daily business of public safety officials, but the ability to migrate these services to the NPSBN is a significant factor in the network's value proposition to local units of government. As noted above, meeting this need would require neutral transport via the NPSBN.

4. The network MUST provide standardized two-way interfaces for NG911 including call origination as well as media delivery from an outside caller.

As an outstanding issue, there is not yet a common and nationwide architecture established for NG911,[1] and the solution to that problem is far outside the scope of the NPSBN. However, as a companion effort to the NPSBN, it is critical that end-to-end RFEA multimedia may seamlessly flow from the caller, to the PSAP, and to field units as necessary with full integrity of emergency data.

For non-response public safety personnel, the NPSBN must support 911 and NG911 call origination to the full extent that any commercial network would. Typically, a responder would use an "emergency button" to reach a dispatcher directly during an emergency; non-response personnel, however, would more likely send an RFEA.[2]

5. Additional clarification is needed for Recommendation 1.4.1 (6), "home page".

The Advisory Board recommends that a "home page" application *should* be supported by the NPSBN. A home page is a REQUIRED feature because network health information is a substantial responder safety concern.

[1] Generally, the NENA i3 model is most supported and is supported by Minnesota.

[2] "Request for Emergency Assistance"; e.g., dialing 9-1-1.

Additionally, the term "home page" is interpreted to mean the ability for a user to check the health of the network as well as receive any important announcements based on the user's current location. To use the term "home page", one implies that this need is met by a web site accessed via web browser. While a web site is certainly one very good means of performing this type of inquiry, it is critical that the NPSBN provides a network status API so that custom applications and outside systems may query the status of the network and take the appropriate action. For example, a device may have an indicator programmed into the operating system GUI that indicates the health of the network and/or a specialized mobile app that could provide a detailed readout. Or, devices may be configured to abandon attempts to connect to the NPSBN if the device anticipates not having a reliable connection to it based on network health data. This API should be accessible over the public internet so that roaming users may access the API when on outside networks (such as if the NPSBN fails at a location).

6. Per Recommendation 1.4.1 (9), the NPSBN MUST support users outside of their normal jurisdiction to connect to local/home packet data networks.

The Advisory Board recommends that users outside of their normal jurisdictions *should* be able to access their home networks; it must be REQUIRED that users are able to do so. To not support this functionality is contradictory to the spirit of seamless nationwide mobility.

Users outside of their normal jurisdictions may have a significant impact on the performance of the network, as their traffic would be backhauled further than a user who is in his or her normal "home" jurisdiction. These "mobility" users should be subject to traffic priority as is appropriate.

7. Per Recommendation 1.4.1 (10), the NPSBN should natively support a robust multimedia communications suite, and not specifically or exclusively SMS/MMS.

The Advisory Board recommends that the NPSBN *should* support SMS and MMS. There are comprehensive multimedia solutions for communications available within or as companion pieces to 3GPP specifications, such as GSMA's RCS,[3] that fully address these needs and more while still interoperating with legacy services like SMS.

8. Per Recommendations 1.4.6 (28)-(36), the NPSBN MUST provide accurate and up-to-date information on network coverage, performance, and plans.

It is worth noting that, in the end, users of the NPSBN will predominantly be first responders acting on behalf of a unit of local government. Funding decisions made at the local level—such as when, or *if,* to migrate certain communications to the NPSBN, or which services to migrate to it, will be based specifically on factors like coverage, throughput, cell-edge performance, modulation zones, and others. Without accurate and up-to-date information on these factors, local decision-makers cannot make informed decisions for their stakeholders, and

[3] *See* http://www.gsma.com/rcs/. The State does not specifically endorse the Rich Communications Suite or Joyn brand, but offers it as an example of a holistic and comprehensive approach to the generic problem of multimedia messaging.

it is unlikely that many public safety entities would want to risk migrating communications to a national network that they have no detailed specifications for.

For example, it is the experience in Minnesota that communications interoperability is significantly enhanced by local units of government migrating primary public safety radio communications to ARMER.[4] Local governments have been very interested in coverage and service metrics when evaluating whether to migrate to the ARMER system. Without current and detailed information for the system and without the State's willingness to address design concerns, we would have been unable to make the case for ARMER and would have had significantly reduced participation in the ARMER program and generally reduced communications interoperability in the State.

9. Per Recommendations in 4.1.8, the NPSBN should utilize IPv6 to the fullest extent possible for internal functions of the network.

As acknowledged by the Advisory Board, migration of all IP networks to IPv6 is inevitable. To that end, the NPSBN should utilize IPv6 to the fullest extent possible for all internal functions of the network. In order to interact with external networks, the network and its devices MUST support dual-stack IPv4v6, as most or all networked devices do today, but only expressly for the purposes of interworking legacy systems or throughout the global migration to IPv6.

It is noted that many of the basic value-added features of IPv6 outside of address expansion, such as IPv6 IPSec, have more or less been rolled into IPv4.

10. Per Recommendations in 4.2.2, remote device management and configuration MUST be supported by the NPSBN and Firstnet administrative procedures.

It is critical that national network managers, presumed to be working under Firstnet, as well as local network managers, both have the ability to remote manage and configure devices on the NPSBN.

The ability to stun or kill any stolen, rogue, or lost devices is a basic security feature whose value should be self-evident.

Beyond that, the ability to remotely manage and configure devices otherwise can introduce significant operational efficiencies over today's land-mobile radio networks that generally require radios to be taken out of service for configuration. Commercial carriers routinely push OS updates for Android-series mobile devices, for example. Note that local applications or OS updates (if the mobile OS version is not uniform across the entire network) would be supported as a matter of course by a content-agnostic, neutral transport network.

[4] ARMER is our statewide, trunked P25 land mobile radio system providing a baseline level of mobile coverage county-by-county throughout the entire state.

11. Per Recommendations under 4.3.4, defined APIs for common functions are a critical output of the network and for Firstnet.

The fundamental building block of communications interoperability is the ability to enable two entities to interact, such as two devices that are operated by individuals. In order for devices to interact, they must be able to make a connection.

Many of the connection-related communications interoperability problems of land mobile radio's past are a non-issue on the NPSBN by merit of every device using the same air interface, network, basic specifications (3GPP), datagram (IP), and frequencies. However, applications running on devices cannot make a connection unless the APIs for them are clearly defined to applications developers.

There will be a number of functions, such as push-to-talk, which will be ubiquitous as requirements throughout the entire user base. As such, these functions should have defined APIs, approved by Firstnet, and these same base APIs should be a required components for devices and applications on the network. There should be **no obstacles or barriers** to interacting with information on the network by one who is authorized to do so.

12. Per Recommendations under 4.8.3, security features built-in to 3GPP specifications address most security needs for public safety.

It is noteworthy that consumers use commercial LTE networks for highly security-sensitive activities such as mobile banking transactions, and 3GPP specifications have been developed to meet those security needs. The Advisory Board has provided a very good baseline for network security that meets the needs of Minnesota.

13. There is uncertain value in the Trusted Delivery Process outlined in Appendix 2.

The Advisory Board's Trusted Delivery Process, as outlined in Appendix 2, has uncertain value to the NPSBN. It is not evident—either in the Advisory Board's abbreviated recommendation for it or in available published literature—that there is a history of OEMs or software providers including malicious code or other "back-door" mechanisms that put public safety network equipment at additional risk for sabotage or damage through negligence. Furthermore, it is not evident that an independent assessor would be any less likely to be responsible for opening the network to such intrusions and vulnerabilities than an OEM or software provider.

The state of Minnesota is pleased to have had the opportunity to comment on the Advisory Board's recommendations, and with only minor exceptions as outlined above, endorses them in their entirety.

Respectfully Submitted,

Jackie Mines

Jackie Mines, Director

Minnesota Department of Public Safety
Division of Emergency Communication Networks