MINNESOTA DEPARTMENT OF PUBLIC SAFETY



Alcohol and Gambling Enforcement

Bureau of Criminal Apprehension

Driver and Vehicle Services

Emergency Communication Networks

Homeland Security and Emergency Management

Minnesota State Patrol

Office of Communications

Office of Justice Programs

> Office of Traffic Safety

> > State Fire Marshal

Emergency Communication Networks

445 Minnesota Street • Suite 137 • Saint Paul, Minnesota 55101-5137 Phone: 651.201.7547 • Fax: 651.296.2665 • TTY: 651.282.6555 www.ecn.state.mn.us

November 1, 2012

Re:

To: National Telecommunications and Information Administration

NOTICE OF INQUIRY Development of the Nationwide Interoperable Public Safety Broadband Network

Docket No: 120928505-2505-01 RIN: 0660-XC002

Please find attached Minnesota's response to the National Telecommunications and Information Administration's Notice of Inquiry dated October 1, 2012.

This filing was prepared for the Interoperable Data Committee of the Statewide Radio Board, who upon a majority vote of its members endorsed this filing on October 24, 2012.

Our state and its SIGB are pleased to have the opportunity to provide its input on this very important issue.

Respectfully,

Sh C.

T. John Cunningham Interoperable Data Committee Co-Chair

Fire Chief & Director of Emergency Management City of Elk River, Minnesota

Wite Bisvolel

Michael J. Risvold Interoperable Data Committee Co-Chair

Chief of Police Wayzata Police Department

EQUAL OPPORTUNITY EMPLOYER

Background information on filing party:

The Interoperable Data Committee (IDC) is a subject matter committee established under the Minnesota Statewide Radio Board (SRB). The SRB is Minnesota's Statewide Interoperability Governing Body (SIGB) and is representative of all stakeholder organizations throughout the state. The IDC was established under the SRB in 2012 to address topics of interoperable data, including the public safety nationwide wireless broadband data network. The IDC's membership includes representatives from public safety agencies, state and local government, tribal government, private partners, commercial carriers and service providers, and public utilities.

The SRB has taken a strong interest in wireless broadband for years, having participated in or commissioned multiple studies investigating wide-area public safety broadband networks since 2009. Most recently, the state of Minnesota and the SRB published the Minnesota Public Safety Wireless Data Network Requirements Study. This study provides a high-level assessment of the state of Minnesota's needs and anticipated cost to build out a statewide LTE network for public safety. This study should be considered an early foundational model for assessing public safety broadband network needs throughout the nation.

For more information, including a full roster of members, please see <u>https://dps.mn.gov/entity/srb/Pages/default.aspx</u>.

Priority, quality of service, and preemption:

FirstNet should delegate management of priority, quality of service, and preemption to the SIGBs to establish rules based on their individual requirements as well as the requirements of their stakeholders. In this case, the customer's requirement is that features for priority, quality of service, and ruthless preemption are supported by the network. These features are built-in to LTE and meet public safety's requirements.¹

Some of these features will be configured on a per-eNodeB basis, per-device basis, per-application basis, per special role basis, and/or on a per-agency basis and may be configured dynamically in response to emerging incidents. It is unlikely that there will be a universal single configuration of the myriad traffic management features included in LTE that would meet the needs of public safety agencies throughout the country. Therefore, the specific configuration of these features, outside of those that are standardized,² should be delegated to the governance structure in each state based on that state's operational standards and the nuances of each regional deployment.

¹ Features including Access Barring, Access Reservation, Access Control, Allocation Retention Priority, QoS Class Identifier, Guaranteed/Maximum Bit Rate, and others meet public safety requirements to assign and manage priority and bandwidth over a shared wireless broadband data network.

² E.g., 3GPP has standard Access Classes, and has assigned classes 12-14 to public safety. FirstNet may wish to standardize other priority management features after consulting with stakeholders.

FirstNet should consider delegating dynamic control of network priority and pre-emption to PSAPs. During emerging incidents, technical staff at a PSAP may want to reconfigure priority for specific roles or applications on the network to ensure high-priority activity has guaranteed bandwidth. To support this feature, FirstNet should consider offering a network service in which applications operated by authorized users can adjust dynamic priority values.

Local control of dynamic priority is important to facilitate network sharing agreements. For example, consider the use case of a utility partnership. Under a utility partnership, Supervisory Control and Data Acquisition (SCADA) messages would have high traffic priority during day-to-day use, while metering and administrative multimedia communications for field users would not require high priority. During a major weather event, field users for the utility would be elevated to high priority to support their lifesaving emergency work, because they are acting as first response entities through the duration of that incident. The PSAP controlling communications for that incident would able to make a reasoned, intelligent decision about how to assign priority at which sites during that incident and could do so on the fly. Without high priority for SCADA and incident traffic, a utility might not be interested in using the FirstNet National Network (FNN); while without the ability to meter and control traffic, a public safety agency might not want to allow utility traffic on a public safety network. In this case, the ability for a local entity to dynamically control priority is foundational to the viability of the partnership.

Deployment strategy:

FirstNet could reach operational capability as quickly as possible by focusing first on its core infrastructure and services, and the (Radio Access Network) RAN second. There will be some period of time before FirstNet will actually begin deploying its RAN in earnest in most states. FirstNet must first finish consulting with each state before it can deploy the RAN, and the states must complete gathering requirements and forming governance under the State and Local Implementation Grant Program (SLIGP) before they are prepared to consult with FirstNet. The actual buildout of the FNN may well take years to complete.

In the meantime, FirstNet should deploy its core infrastructure as soon as possible and begin offering FNN services on it. Wireless users can access the FirstNet core network through private data networks, or by roaming on commercial carriers, until FirstNet deploys its RAN. Fixed users (such as PSAPS) could enjoy the interoperability benefits and services provided over the FNN immediately, as their access to the network is not dependent on the RAN. This approach removes RAN deployment from any agency's critical path to basic FNN services. User agencies would be able to procure devices and applications over an extended window as their budgets and project schedules allow, and to perform training well before the network is deployed in their area. Additionally, this strategy creates a sustainable marketplace which will encourage application developers and manufacturers to develop new products, speeding the availability of mature products in the market.

In building its RAN, FirstNet should utilize existing infrastructure to the fullest extent possible in whichever way validates its business case base in the markets FIrstNet invests in. FirstNet should partner with commercial carriers, public safe agencies, Critical Infrastructure providers, broadcasters, and others on the basis of efficacy, value, and ability to meet user requirements.



Local enhancements:

FirstNet should consider a model in which user agencies may directly invest into and make upgrades to the network. There will be areas where FirstNet's basic offering will not or cannot provide coverage. In these areas, user agencies should be able to make improvements to the network with the stipulation that these agencies are responsible for maintaining those elements of the network.

As a reference point, Minnesota has successfully employed the Local Enhancement model with ARMER. In ARMER, network components are owned, operated, maintained, and controlled by whichever entity has purchased and installed them. The state backbone provides a baseline level of outdoor coverage. Where user agencies require more sites, such as where they require enhanced indoor coverage, the agency builds and maintains those sites as shared, interconnected elements of the overall network.

There are many benefits to the Local Enhancement model. It can reduce potential capital and operational expenses for FirstNet. It enables user agencies to meet specific and occasionally esoteric or emerging needs. The Local Enhancement model reduces incentives that a state would opt-out, because a state could use its own funding to address whatever issues it has with FirstNet's proposal that give it cause to opt out. The Local Enhancement model strengths governance, because stakeholders can have real and tangible investments in a shared communications network. For potential FNN Local Enhancement pilot projects, FirstNet could consider public safety LTE BTOP recipients and other early build-outs.

Public safety applications:

FirstNet must provide an environment which encourages innovation and introduces no obstacles to application development. To that end, FirstNet could embrace many of the factors which have contributed to the massive boom in application development in the commercial mobile sector.

FirstNet should focus its application strategy on services, and not discrete end-user applications or mobile operating systems. The network should be application and operating system neutral. For example, FirstNet could offer a public safety voice service with a standardized interface, which various vendor or in-house applications could utilize to send and receive voice over the network. This approach will allow many vendors to provide innovative applications and allow public safety agencies to reap the benefits of market competition. FIrstNet's focus on services will also allow individual public safety agencies to potentially develop new applications in-house, and share them with interoperability partners throughout the entire nation.

A focus on services will ensure the highest amount of interoperability on the network. By providing services on the network that are universal to all users, FirstNet can passively force application developers and manufacturers to provide solutions that work with that FirstNet's service. Developers will not have to test with one another; so long as the application successfully works with FirstNet's interface, it should work with every other application that uses that service. Vendors and users can focus on features and the end-user experience, instead of which product interoperates with which other product.

FirstNet should not operate an "App Store" for end-users. The App Store model, which as mentioned in the NTIA's NOI is assumed to refer to iOS App Store or Android Market, is not appropriate for FirstNet. Public safety

devices on the network should be considered part of the user agency's enterprise fleet, and managed by its technology staff per the policies of that organization. An App Store delivery system implies a mechanism through which an end-user may choose and install applications that they like from a catalog, which is not appropriate for any enterprise system (unless that catalog is controlled by the enterprise), and it is absolutely not appropriate for first responders, where standardized approaches to training and consistency in user equipment is paramount.

FirstNet might consider operating an application delivery system, which can centrally store and deliver binaries to end-user devices. Smaller or isolated agencies that are not part of a large enterprise could use this service to gain access to basic applications. Agencies should not be forced to use such a service, as large enterprises will prefer to manage application delivery and updates on their own. This is separate and distinct from an end-user App Store in that it provides an application delivery service, but not necessary an ala carte storefront.

FirstNet may have to review and certify applications for use on the FNN. It may have to perform code-reviews and ultimately sign code, and if so, any device OS on the FNN would have to be configured to execute only signed code. If this is the case, FirstNet should provide a service where enterprise IT managers can retrieve the most recently published binaries. FirstNet may also consider a compliance assessment program, where it evaluates applications work with the services proposed above. However, curating and testing is a time-consuming and expensive process. Not only are associated costs passed on to subscribers to the service, but any time devoted to certifying a particular bug fix or patch delays the delivery of that fix to end-users. If FirstNet elects to adopt a certification program, it should carefully consider how that program affects end-users and user agency budgets and exercise restraint accordingly.

FNN's business case:

FirstNet should ensure that it can ultimately offer a sustainable business case while fully meeting stakeholders' defined requirements.

Stakeholders in Minnesota operate with the basic assumption that FirstNet will operate like a commercial cellular carrier. However, if the FNN is built to public safety coverage, resiliency, and surge-handling requirements to the extent that it is a mission critical network, the FNN could very well be a far more expensive network to deploy and operate than any consumer-grade network. Based on what are presumably high operating expenses and a relatively small pool of users, the FNN will require relatively high average revenue per user, compelling and innovative partnerships, or some combination of both.

There are numerous options available to FirstNet to make a business case. For example, FirstNet could reduce its expenses by reusing existing public safety or utility infrastructure which should be available to it at little or no cost depending on arrangements made with user agencies.³ FirstNet should allow direct use of the network by

³ See Minnesota Public Safety Wireless Data Network Requirements Study (2012). This study found that approximately 3/4 of Minnesota's public safety coverage needs would be met by installing LTE equipment on state-owned and local enhancement ARMER sites. ARMER is Minnesota's statewide, trunked P25 radio network operating in the 800 MHz band and is used by the vast majority of public safety officials in the state for primary radio communications.



non-first responders entities, such as critical infrastructure utility entities, educational institutions, public transit, and general government . Any use by non-public safety entities, and any leasing agreements executed within the state, should be done under the sponsorship of the SIGB. FirstNet could enter into partnerships with private entities, such as rural telcos, to provide fixed or mobile wireless service to areas where providers cannot, on their own, make the business case to provide high speed broadband internet access. 3GPP LTE/SAE standards provide robust technical features to accommodate these and many other business strategies to make these and other partnerships possible without interfering with or blocking public safety traffic.⁴

(END)

⁴ For example, the LTE network can assign ruthless pre-emption and guaranteed bearers to public safety users over the air. During a major incident, "secondary" users such customers of a partner telco would experience service degradation or interruption to accommodate public safety traffic.