



April 12, 2011

Ms. Jennifer Manner  
Deputy  
Public Safety and Homeland Security Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, DC 20554

RE: PS Docket No. 06-229; WT Docket 06-150; WP Docket 07-100; FCC 11-6

Dear Ms. Manner:

On behalf of the National Association of State Chief Information Officers (NASCIO), I am writing to submit comments in response to the Notice of Proposed Rulemaking posted in the February 24, 2011 *Federal Register* regarding the development of a technical interoperability framework for nationwide public safety broadband network operating in the 700 MHz band. NASCIO represents the state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia. Thank you for the opportunity to comment on this NPRM.

In response to the NPRM, it is important to understand the service business model of the state CIO organization. Operating under the leadership of the state CIO, the majority of state enterprise IT agencies are structured in a similar fashion and procure services on behalf of agencies and other public entities consolidating the services into service offerings on a chargeback basis, user fee or comparable model of delivering services. Typically, the executive branch agencies are “customers” that purchase data center, communication services, network, e-mail, system backup, storage or other unit services under a published rate or pro-rated assessment method. Central state IT organizations acquire, manage or operate a suite of communications technology services to deliver voice, data and video services. Generally these services are procured and sourced from private sector carriers/providers under a competitive solicitation. These services typically include local and long distance voice, wireless cellphone, smartphone services (voice, text and web access), interactive voice response (IVR) and other contact center functionality (e.g. predictive dialers, recorders, workflow/workforce management), Internet services, local area networks, wide area networks, “last mile” connectivity, virtual private networks, voice over IP (VoIP), video and audio conferencing and digital microwave.

On a daily basis, State Chief Information Officers support public safety activities through the provision of the statewide communications infrastructure. State CIOs are moving state networks to IP based communications. Our country’s local, state, tribal, and federal law enforcement, fire, medical, and other emergency professionals must have access to the most modern and reliable wireless broadband technologies to communicate with each other and with federal officials across agencies and geography during emergencies. In addition, the ability for public safety to have seamless nationwide roaming capability on a wireless broadband network that is hardened to public safety requirements is achievable and essential for public safety to meet its ever-increasing responsibilities.

NASCIO • 201 East Main Street, Suite 1405 • Lexington, KY 40507  
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: [NASCIO@AMRms.com](mailto:NASCIO@AMRms.com) • W :: [www.nascio.org](http://www.nascio.org)

NASCIO supports the establishment of a national interoperable mobile wireless broadband network that will improve our nation's homeland security and provide first responders with new voice, video, and data communications technologies that are urgently needed. As a strong advocate for enterprise architecture and open standards, NASCIO supports a uniform foundation for public safety communications. Rather than relying on slices of disparate spectrum for public safety, a nationwide architecture is needed to reduce complexity, promote advanced services and direct future investments toward true interoperability.

### **The Need for a Unified, Multi-purpose Broadband Network for Public Safety**

NASCIO applauds and supports the efforts to date by the Federal Communications Commission to conceptualize a nationwide broadband framework for public safety. Architecting and future-proofing a communications interoperability framework for the nation must continue to be at the forefront for federal as well as state jurisdictions to improve the overall effectiveness of public safety and first responder operations at all levels.

NASCIO endorses the following architectural principles:

- ✓ Long Term Evolution (LTE) as a common technology platform for all public safety broadband networks
- ✓ A multi-purpose technology platform that unifies mobile voice, video and data requirements seamlessly across all participating jurisdictions
- ✓ Nation-wide ubiquitous coverage with seamless handoff between varying generations of wireless service (2G, 3G and 4G)
- ✓ A common air interface to ensure nationwide interoperability, specifically 3GPP standard, E-UTRA, Release 8 or higher, and associated EPC
- ✓ Backward compatibility between all subsequent releases from Release 8 and onwards to ensure technical baseline for interoperability is preserved
- ✓ To ensure interoperability when roaming across networks, common air interface must include Uu, S6a, S8 and S9 interfaces
- ✓ A technology platform that is optimized for maximum spectrum efficiency

In addition, NASCIO strongly recommends the following core elements be considered when finalizing the overall framework:

1. NASCIO strongly believes that a "Network of Networks" concept for achieving nationwide interoperability is not sustainable. A unified backbone with geographically-placed cores strategically located throughout the country would accelerate the path toward nationwide interoperability while minimizing the capital investment required building out the network cores. With this model, jurisdictions could focus their dollars on building the eNodes to ensure coverage within their jurisdiction while having a clear roadmap for how to connect to the nearest core to achieve inter-jurisdiction interoperability. The location of the cores could mirror the FEMA Regions as an example. States would be responsible for the backhaul transport from their eNodes to the FEMA core which they're assigned to. This provides a clear division of responsibility between the federal government and states, and minimizes the number of network cores, which would go a long way to reducing interoperability complexity in the future.
2. NASCIO strongly believes that future federal grants, PSIC or BTOP funding opportunities should be at the state level. A state "enterprise" view is an imperative. This approach would guarantee the most effective use of taxpayer dollars to build a state-level interoperability capability.

Exceptions may be considered for large metropolitan areas such as New York City, Boston, Chicago, Los Angeles and select jurisdictions. Since E-911 surcharge fees are assessed and collected at a state level, designating state-level jurisdictions with the responsibility of ensuring state-wide interoperability would position states to leverage the E-911 surcharge to sustain intra-jurisdiction interoperability requirements.

3. NASCIO supports the reallocation of the D-Block to public safety and the establishment of regulatory process and structure to construct a national interoperable mobile wireless broadband network that will improve our nation's homeland security and provide first responders with new voice, video, and data communications technologies that are urgently needed. With the growth of mobile devices being used by the public and switch to NG 9-1-1, reallocation of D-Block is needed.
4. The FCC should not restrict "secondary" users or federal users for using the network during non-emergency.

### **Public Safety Broadband Network Coverage Requirements and Reliability**

In developing standards for coverage requirements and liabilities, the Commission should consider many factors that will drive timely completion of the network. The network capabilities will need to be static, with an ability to become dynamically provisioned when requested, allowing interoperable communications through the lifecycle of an emergency event response to recovery while maintaining lower cost of operations generally. These comments provide guiding principles that can lead to a better framework for the public safety network coverage requirements.

#### **1. Achieve Interoperability Quickly by Expanding Coverage Through Minimally Defined Bandwidth Services**

The current state of the public safety networks in the US varies with many having narrowband voice and data capabilities and very few with video services that are fully interoperable. Given that the baseline requirement is Long-term Evolution (LTE), this will require build out in many rural, less densely populated areas.

The Commission should consider expanded coverage through minimum bandwidth services and applications in a layered approach by initially setting interoperability standards first for deploying voice and data. This approach would encourage more rapid build out of the overall network, by reducing upfront cost. Layering more costly services into the requirement over time would assist and encourage many smaller entities.

#### **2. Bridge Older Technologies in the Public Safety Network in Remote Areas**

For service in extremely isolated or rural locations be achieved, at least initially, by "bridging" older technologies into the systems as an initial approach as absolutely necessary. An aggressive timeframe for bridging these technologies is recommended with alternative technologies to be in place regionally to move assets in to the area in the likelihood of a widespread disaster scenario or other emergency need. Bridging the older technology will require good standards such as failure rates, limitations on voice and data transmission, reliability measures and lifecycle cost. For this to become a reality an assessment of the bridge technologies and the cost of ownership are warranted. Also, timelines should be established for minimal standards established by FCC.

The bridge technologies will need to be considered gap technology with public safety standards incentives in place to reach full LTE deployment capabilities. This approach strengthens the static network that supports most emergency situations but not the catastrophic events that will require a

more dynamic network design that will allow first responders the best communications services anywhere in the US.

**3. Establish Requirements or a Decision Matrix for Areas that Host Critical Assets and Industries**

Many rural locations host critical infrastructure facilities like power plants, fuel refineries and data centers. Limiting the criteria to geography, population mass or highways is essential, but should include critical assets. Critical assets throughout the United States will require the public safety network requirements to cover these areas no matter where they are in the country. A dynamic decision matrix, including these critical assets along with population and other demands is needed. This will protect against missing an important element of any future requirement.

**4. Incentivize Local Governments and Private Companies to Share Resources**

A shared resource approach should be encouraged to share telecommunication assets. A methodology and regulations should include looking at regulatory barriers. The evolution to a fully developed LTE system will expand “farther, faster”. By instituting aggressive requirements local governments will be encouraged to collaborate and partner in the development of the network.

The FCC should consider establishing requirements for what the core network will be able to provide which would be under a federal governance structure. The telecommunications tributaries of the shared resources assets will need to reach the established federal points of presence or network centers. These centers will be placed strategically in areas and become the junction boxes for local and regional connection points. These facilities can allow for on-site or virtual access presence from their own geographically locations. This approach provides flexibility that broadband allows by extending resources to public safety responders without having to go through central dispatch centers. In addition, satellite communications could be facilitated for catastrophic events. The size and scope of the federal baseline network and shared lesser telecommunications assets becoming connected to it through rigorous requirements is an approach that should be investigated.

The benefits of shared resource network centers will allow for economies of scale on equipment deployments promote public safety local and regional collaboration, and multi-entity efforts. By introducing expansive federal procurement vehicles and processes this will allow local and regional entities to utilize equipment, and facilities in new ways. The cost savings for this approach would be significant and allow the FCC to reach its full deployment objectives quicker. By example, one “center”, shared by 3 or 4, may cost twice that of a single facility to implement and operate; however, the net savings allows many to participate at lesser local cost. Savings from this arrangement, where it may be possible, could then be deployed to better provision the network, allow for satellite backup usage while the network is expanding, and even provide operational funding to encourage a more rapid adoption and build.

**5. Reduce Barriers Such As Tariffs, Regulatory, Funding and State Border Issues That Can Prevent Development of the Network**

Generally some states and local governments still have restrictions like tariffs prohibiting cross boundary cooperation. Some localities, like Sarasota FL, have excellent models where they reach out to surrounding areas and provide, for a fee, certain technology-based services. Where restrictions remain, opportunities such as this are not feasible. One element to consider is to reach “further, faster” and with less cost, help enable change, or remove, these local, state and federal obstacles.

Requiring all services and applications by all communities will create a significant funding barrier to many entities. Should we address the potential to scale based upon the population, geography, etc. scale for some period of time? The decision matrix referenced should guide “who needs to do how

much by when” (e.g. – even the small jurisdictions in the threat zone, have to adopt and deploy voice and low data).

**Conclusion**

We urge the FCC to consider the recommendations and comments made by NASCIO and its members. Thank you for considering our comments. Please contact Pam Walker, NASCIO Director of Government Relations at 202-624-8477 or [pwalker@amrms.com](mailto:pwalker@amrms.com) if you have any questions.

Sincerely,

A handwritten signature in blue ink that reads "Kyle Schafer". The signature is written in a cursive style with a prominent initial "K".

Kyle Schafer  
NASCIO President  
Chief Information Officer, State of West Virginia