Fairfax County, Virginia

Response to National Institute of Standards and Technology Request for Comments

October 12, 2011

DRAFT

Table of Contents

1. Introduction 3

2. National Institute of Standards and Technology Comments 4

3. Conclusion 6

1. Introduction

Fairfax County is the largest jurisdiction by population in the Commonwealth of Virginia, with 1,037,605 citizens living within its 407 square miles. Public safety services are provided by 7 local law enforcement agencies, the Fairfax County Fire Department and numerous state and federal agencies. Interoperable communications in this region are both challenging and critical, but with the creation of the National Capital Region with 19 other local jurisdictions, interoperability has become reality.

Fairfax County first responders rely heavily on the existing radio network for voice communications that does not have broadband data capability; and commercial networks for mobile data capability that has been unreliable for data-intensive first responder field operations. With the allocation of the public safety 700 MHZ broadband spectrum, there is now the opportunity to provide responders with a secure, reliable, interoperable, public safety grade broadband wireless network.

Pursuant to Federal Communications Commission (FCC) requirements, the County has identified public safety interoperable broadband services as a priority and on June 28, 2010 filed a waiver to continue efforts to deploy a network as quickly as possible in the 700 MHz public safety broadband spectrum. The County's private fiber enterprise network will meet the technical specifications the FCC has proposed in the *Third Further Notice* and the September 4, 2009 National Public Safety Telecommunications Council ("NPSTC") 700 MHz Broadband Task Force Report and Recommendations ("NPSTC Recommendations")[3] and can be integrated into a future interoperable public safety broadband network.

Fairfax continues its efforts to deploy manage and maintain a 700MHz wireless broadband network that is integrated with the 700MHz wireless broadband nationwide network. Fairfax strongly believes that public safety communications network (s) must be controlled by state and local governments. All incidents start out local and in a new, converged voice, video and data environment, local PS leaders must have the ability to make real-time network priority changes and when necessary preempt users without unreasonable escalation procedures envisioned by the FCC in 2007. Fairfax is pleased to provide the following comments to the National Institute of Standards and Technology request for comments. We look forward to working in strong partnership with the federal government to implement our network communications plans.

2. National Institute of Standards and Technology Comments

Resiliency: The ability of operable systems to recover from mishap, change, misfortune, or variation in mission or operating requirements.

This is a very important feature for a PS communications. In particular, we are concerned about national or regional Public Safety network outages. As a matter of resiliency, we have to have an architecture that minimizes large scale outages, and that can only come from having multiple Cores. A nationwide network, which we view as a "Hybrid" of a national network and State and Local networks; needs to have more cores than commercial carrier networks, but not as many as current Land Mobile Radio networks. A “Hybrid" network architecture will meet PS' resiliency requirements and minimize major outages for Public Safety communications in the future.

Prioritization: The ability to prioritize network traffic based on assigned priority schemes.

There is a definite need to have software that sets certain baseline priorities on our networks. However; there is no way to pre-program priorities for **every** type of incident/situation. State and Local governments must be able to dynamically manage messaging and data on an incident by incident basis in real-time.

Meshing: A type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other sensor nodes, and propagate the data in the network.

The ability each authorized device to communicate with all other authorized Public Safety devices or networks is another important key feature that is essential during network communication outages. Care should be taken in development so that we do not create a proprietary set of solutions that will hinder operations and compatibility, or be too costly to afford.

Compatibility with Commercial Infrastructure: The utilization of a variety of commercial services when public safety is in areas not covered by the public safety broadband network.

This is must have feature. We cannot afford to build out a Public Safety Broadband Network at the level of resiliency, self-organizing, QoS, configuration, prioritization, and adaptability needed for Public Safety networks in every area of the county. It is critical that we remain interoperable amongst local jurisdictions and the commercial carrier partners. Our compatibility with the commercial carriers is one of the keys to the success of the nationwide network.

Network Sharing: The shared use of infrastructure between commercial and public safety users.

This is another key feature. The ability to share networks will minimize the cost of deployment, but we should first try to leverage investments of our local government's vast amount of existing infrastructure, such as towers, fiber, microwave, and facilities. The significant portion of our interoperability investments over the past 10 years have gone to improving local and state infrastructure for LMR communications. We should first reuse this infrastructure, and then leverage the commercial carrier's infrastructures where necessary.

Multi-Modal: The ability of the network to support voice, video, data, and multimedia simultaneously.

This feature is an important need for Public Safety. We need to have Voice, Video, and Data features all working together. The ability to use these features simultaneously across the network is critical for Public Safety entities.

Scalability: The ability of a system, network, or process to handle growing amounts of work in a graceful manner or its ability to be enlarged to accommodate growth.

We must be able to supplement our networks with solutions to help with capacity in areas where capacity is low and/or when our responders are out of our base coverage areas. This is needed even if Public Safety is awarded the D-Block Spectrum.

Standardized Common Interfaces: Protocols, Application Program Interfaces, application platforms, radio capabilities that allow for competitive provisioning.

This feature is inherently critical to the success of the network. There should be standards set on protocols, application program interfaces, application platforms, and radio capabilities. However, those standards should not be so stringent that they inhibit innovation. It is very important to strike the right balance. We need to set up a "Swimlane of Standards" that will encourage innovation while maintaining the integrity of all the components of our nationwide network.

Uniform, Universal Access: The ability to access the network and data anywhere at any time through any device.

This is also an important feature to achieve full interoperability. However, it is essential that only authorized devices have access to Public Safety networks and data.

3. Conclusion

The distinct need for a private broadband wireless network for Fairfax County, Virginia and for all independent jurisdictions throughout the country is both essential and fundamental. The three fundamental drivers that justify the public safety broadband network are: to improve data throughput, to provide network availability, and to improve network reliability. Underlying these drivers for a broadband network is that the network must be cost effective so that it can be shared by critical agencies, first responders, public service, transportation and other critical infrastructure providers. The Fairfax County public safety community will use the new wireless broadband network to improve its day-to-day communications and emergency response. As stated earlier, we believe that a Hybrid Nationwide network that leverages State and Local private networks and a nationwide network build out in non-private State and Local network areas is the best approach to addressing PS broadband communications needs nationally. We also feel that a "Balanced" National Governance is needed to standardize network build out, maintenance, operations and control. The Federal Government is critical to this process but without State and Local network deployment decision making authority and state and local network control; we will not be able to achieve network reliability and availability required nor the improved incident management response our first responders need and deserve.