Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of:	)	
	)	
Service Rules for the 698-746, 747-762 and 777-792 MHz Bands	)	
	)	WT Docket No. 06-150
Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band	)	PS Docket No. 06-229
	)	WP Docket No. 07-100
Amendment of Part 90 of the Commission's Rules	)	
	)	

COMMENTS OF
THE NATIONAL PUBLIC SAFETY TELECOMMUNICATIONS COUNCIL

The National Public Safety Telecommunications Council (NPSTC) submits these Comments in response to the Commission's Fourth Further Notice of Proposed Rulemaking (Fourth FNPRM) released January 26, 2011 in the above-captioned proceeding. In the Fourth FNPRM, the Commission seeks comment on the architecture and rules most appropriate to "further promote and enable nationwide interoperability among public safety broadband networks in the 700 MHz band."[1] As addressed in the comments herein, NPSTC supports a nationwide architecture with provisions for regional control, together with rules essential to nationwide interoperability. NPSTC cautions against codifying too many detailed rules at this early stage of broadband deployment. Given the many detailed rules proposed, it is likely that a number of the rules would need to be modified based on additional deployment and operational experience yet to come. The multi-year process to do so could further delay the provision of broadband service to public safety.

[1] Third Report and Order and Fourth Further Notice of Proposed Rulemaking, WT Docket No. 06-150, PS Docket No. 06-229, WP Docket No. 07-100, released January 26, 2011

The National Public Safety Telecommunications Council

The National Public Safety Telecommunications Council is a federation of public safety organizations whose mission is to improve public safety communications and interoperability through collaborative leadership. NPSTC pursues the role of resource and advocate for public safety organizations in the United States on matters relating to public safety telecommunications. NPSTC has promoted implementation of the Public Safety Wireless Advisory Committee (PSWAC) and the 700 MHz Public Safety National Coordination Committee (NCC) recommendations. NPSTC explores technologies and public policy involving public safety telecommunications, analyzes the ramifications of particular issues and submits comments to governmental bodies with the objective of furthering public safety telecommunications worldwide. NPSTC serves as a standing forum for the exchange of ideas and information for effective public safety telecommunications.

The following 15 organizations participate in NPSTC:

American Association of State Highway and Transportation Officials
American Radio Relay League
Association of Fish and Wildlife Agencies
Association of Public-Safety Communications Officials-International
Forestry Conservation Communications Association
International Association of Chiefs of Police
International Association of Emergency Managers
International Association of Fire Chiefs
International Municipal Signal Association
National Association of State Chief Information Officers
National Association of State Emergency Medical Services Officials
National Association of State Foresters
National Association of State Technology Directors
National Emergency Number Association
National Sheriffs' Association

Several federal agencies are liaison members of NPSTC. These include the Department of Homeland Security (the Federal Emergency Management Agency, the Office of Emergency Communications, the Office for Interoperability and Compatibility, and the SAFECOM Program);

Department of Commerce (National Telecommunications and Information Administration); Department of the Interior; and the Department of Justice (National Institute of Justice, CommTech Program). NPSTC has liaison relationships with associate members, the Telecommunications Industry Association, the Canadian Interoperability Technology Interest Group, the National Council of Statewide Interoperability Coordinators and the Utilities Telecom Council.

NPSTC Comments

1. Background

The Fourth FNPRM is the latest in a series of proposals and public notices over the last five years related to the 700 MHz public safety broadband network. The regulatory history and work to date in this proceeding underscore that both nationwide interoperability and regional control to ensure systems meet requirements in the respective areas in which they are deployed are the overarching requirements as we embark on deploying the public safety broadband network.

Rules previously proposed in 2006 and adopted in 2007 envisioned a process in which 10 MHz of public safety spectrum would be licensed to one nationwide public safety broadband licensee (PSBL) and combined with 10 MHz of spectrum in the adjacent D block. Under the Commission's original plan, a commercial operator would have obtained the D block spectrum at auction and would build out a public safety broadband network over both the D and PSBL spectrum blocks. The 10 MHz block of public safety spectrum was successfully licensed on a nationwide basis.[2] However, subsequently, when the D block auction failed, the Commission issued a Third Further Notice of Proposed Rulemaking which in general sought to reduce the

[2] Cite PSST license decision

public safety-related requirements for the D block operator.

In response, a number of jurisdictions submitted waiver requests to access the PSBL spectrum block so they can build out a network designed to meet public safety needs in their respective areas. The waiver requests also included recognition of the need for nationwide interoperability. The Commission issued a waiver Order on May 12, 2010 which granted the first 21 waiver requests submitted. That waiver Order set forth interoperability requirements for the 21 waiver grantees. A subsequent Public Notice issued May 26, 2010 and another Order released in December 2010 set additional requirements on waiver grantees beyond those included in the May 12, 2010 Order. While these actions addressed requirements for waiver grantees, they did not address changes to the rules originally adopted in the Second Report and Order.

With those successive actions as a back-drop, the latest Third Report and Order and Fourth FNPRM addresses revisions of the rules for the 700 MHz broadband network going forward. The Third Report and Order mandates in the rules that all public safety broadband networks adopt LTE as the common technology platform, similar to the requirement for LTE in the previous Waiver Order. In addition, the Third Report and Order included a stay of the partnership rules previously adopted which is premised on a mandatory PSBL partnership with the D block auction winner.

The Fourth FNPRM focuses on the overall architecture and proposes many additional requirements "to further promote and enable nationwide interoperability among public safety broadband networks operating in the 700 MHz band." [3] In these comments, NPSTC will focus primarily on recommendations related to the overall architecture and on what would be helpful

[3] Fourth NPRM at paragraph 15

to include in the Commission rules, as well as what would be counterproductive to codify into a rule at this stage of the process.

NPSTC also understands the need for waiver grantees, especially those who have funding, to move forward with deployment without further delays while any overall national-level issues are finalized. The thinking behind the waiver grants was that these early deployments would provide valuable insight and experience that could be leveraged as the network rolls out nationwide and NPSTC still believes that to be the case.

2. Definition of Interoperability

At the outset, NPSTC agrees with the Commission's proposal to modify its rules to adopt the definition of interoperability used by the Department of Homeland Security as developed in the SAFECOM program. DHS and the SAFECOM program have defined interoperability as "…the ability of public safety agencies to talk to one another via radio communications systems – to exchange voice and/or data with one another on demand, in real time, when needed and when authorized."[4]

NPSTC supports this definition for several reasons. First, this definition is not one that was dictated at the Federal level to state and local public safety entities. Rather, given its development in SAFECOM, the definition represents the collective input of multiple organizations each representing various parts of the state and local public safety community. NPSTC supports the Commission in leveraging that collective wisdom. Second, the SAFECOM definition recognizes that not every public safety user needs to communicate with every other user all the time, i.e. such communications need to be "when authorized." Public safety agencies need to maintain control of communications and ensure that incident command structure is in place and followed as needed.

[4] *See* SAFECOM, http://www.safecomprogram.gov/SAFECOM/about/default.htm.

The Commission requested whether this definition of interoperability should apply only to broadband communications or should be extended to narrowband and broadband communications. The definition points to the need to "exchange voice and/or data." Accordingly, NPSTC believes it is very important to consider the inherent capabilities of broadband and narrowband networks, respectively in applying the definition and any rule in which the definition is embodied. For example, the current LTE standard does not support mission critical voice communications but is highly applicable to exchanging data. In contrast, narrowband systems are designed primarily for mission critical voice but do not have the capacity for data in the speeds and volumes that public safety requires. In addition, "data" in the context of public safety requirements for the broadband capabilities could include the transmission of video when needed. Therefore, the spectrum capacity of the broadband network would need to reflect that requirement.

3. Architectural Framework, EPCs and PLMN-IDs

NPSTC supports establishing an architecture that enhances and simplifies nationwide interoperability, and at the same time provides local/regional/state/tribal entities the ability to control the elements and functions needed to meet their respective operational requirements. NPSTC also supports steps to help minimize capital and operational expenses to the extent possible within the context of meeting the above nationwide interoperability and local/state/regional/tribal requirements. In deciding a path forward, all of these goals need to be considered as a whole, not just interoperability alone, meeting local needs alone or minimizing costs alone.

In previous comments, NPSTC noted that multiple public safety agencies within an overall region or in neighboring regions could chose to share an LTE Evolved Packet Core (EPC) to help

reduce costs while still providing operational control.[5] The EPC contains several different nodes responsible for operation of a LTE network. These nodes are physical in nature but can also be logically split out from individual pieces of hardware. In general, this would allow multiple jurisdictions who desire to do so to share the cost of EPC nodes, while still maintaining local control. NPSTC continues to believe that some limited number of EPC cores nationwide should be able to meet these goals and therefore it is an approach we have supported. We do not believe that each and every locality needs to have its own core.

However, as noted on the NPSTC panel at IWCE in March 2011 NPSTC is not recommending that the Commission adopt a specific number of cores as a requirement in the rules. The information NPSTC has provided in recent ex parte presentations is meant to depict a typical approach that NPSTC believes could be viable.[6] Additional discussions between public safety practitioners and industry continue to be held on this point as there are tradeoffs in costs, desired redundancy, reliability, network governance and where various control functions reside, depending on how the public safety broadband network is architected. Regardless of the number of EPCs ultimately deployed, NPSTC believes the most important element to consider is whether the paths chosen provide the interoperability, operational control and level of reliability needed by public safety agencies. Similarly, NPSTC believes that using one nationwide network identification, i.e., PLMN ID could simplify nationwide interoperability as public safety users in one region who travel to another region would not be "roaming" onto compatible networks. All devices would simply operate in all areas of coverage of the public safety common architecture. The only roaming required would be from the public safety network onto commercial networks. This may also help minimize complexity and costs.

---

[5] NPSTC Comments at page 5, submitted July 19, 2010 in response to the Commission's Public Notice DA10-884, released May 18, 2010.

[6] NPSTC ex parte filing in PS Docket 06-229 dated March 4, 2011.

We do recognize, however, that regardless of the number of PLMN IDs deployed, there needs to be a viable mechanism for local/regional/state/tribal public safety broadband operators to be able to control network access in their respective areas and under what priority both local and visiting users have with such access in a given situation. The need for this mechanism supports a key element of the SAFECOM interoperability definition, i.e., communicating "…when needed and when authorized." The LTE standard includes multiple levels of prioritization and provides the foundation upon which these functions can be provided. The use of one PLMN ID would eliminate roaming within the public safety data network, and would provide significant simplification of the nationwide network. All devices would simply operate in all areas of coverage of the public safety common architecture. As noted above, the only roaming required would be public safety users roaming onto commercial networks.

NPSTC recommends that the FCC not regulate the specific number of PLMN IDs, but instead consider the PLMN ID structure as a factor in addressing the overall system architecture to ensure the key goals NPSTC set forth above. Public safety needs flexibility and support from the Commission to plan the development, implementation, operation and governance of the nationwide architecture and an orderly build out of data service to all areas of the nation over time. The architecture and core network will need to be engineered to maximize redundancy, survivability and reliability, minimize backhaul links, maximize local control over the RAN and meet public safety operational needs at the local level.

NPSTC believes it is too early in the process for the FCC to regulate all the technical details of the architecture. There is too great a risk of establishing regulations that inadvertently force the operational characteristics of the network down a path that will not meet Public Safety needs and adds unnecessary duplication and costs to public safety users. Furthermore, restrictions incorporated

into the rules now would likely take several years to remove or modify should they prove to be unnecessary or counterproductive to the deployment of public safety broadband systems designed to meet both operability and interoperability requirements.

Locking down every technical detail in the rules could actually hamper rather than help deployment of nationwide broadband network capabilities needed by public safety. Data rates, coverage and cost are inherently intertwined. Requiring network capabilities on a nationwide basis in the rules could actually prevent deployment of broadband service that could otherwise be well-received in rural areas. It simply may not be possible to fund the deployment necessary to provide the same level of data rates in a rural area as in metro areas, especially at the outset. At this stage, rules should be limited to those essential to providing nationwide interoperability, without preventing current or future innovation that best serve the needs of local, state, regional or tribal public safety entities in the variety of environments different areas face.

4. Network Evolution

The use of LTE as the standard for public safety broadband operations in the 700 MHz band has garnered wide support from the public safety community, the equipment manufacturing industry and commercial operators who hold spectrum in the 700 MHz band. Accordingly, the Commission appropriately adopted LTE as the standard for 700 MHz band public safety broadband and has already specified the required interfaces from the 3GPP LTE standard, release 8. The Fourth NPRM seeks input on how best to manage upgrades to the network as the standard and technology advances beyond release 8. For example, the Commission questions whether to adopt rules to ensure public safety agencies incorporate newer releases of the standard.

NPSTC agrees that evolution of the network is important, but we must first have a network deployed to evolve. The public safety community and the Commission are now five years into the regulatory process for 700 MHz broadband with minimal deployment to date. Therefore, we recommend that the first priority focus be on establishing sufficient dedicated spectrum and funding in Congress and a basic set of rules at the Commission to provide for nationwide interoperability and the requisite level of regional control. It is important to get a baseline set of 700 MHz band public safety broadband capabilities actually deployed, using required features and functionalities of the LTE standard recently adopted, based on technology already available and deployed commercially.

NPSTC does believe that a common nationwide architecture could simplify the issues of implementing release upgrades. It is also our understanding that the process under which 3GPP updates standards requires that new releases be backward compatible with the previous release. Another issue requiring study and testing is the extent to which multiple release versions can co-exist on the common nationwide architecture. However, managing upgrades to the public safety network goes beyond technology and is directly impacted by issues of funding, maintaining uninterrupted operations, etc. Given the public safety network is not yet deployed and neither funding amounts nor mechanisms for operations, maintenance and upgrades have yet been finalized, the best approach to manage migration to future releases of the standard is not known at this time. Therefore, NPSTC believes it is premature to adopt detailed rules for the network evolution process.

5. Voice Capabilities on Broadband

The Fourth FNPRM also asks whether it is necessary to mandate that networks be upgraded to include voice capabilities as voice is supported in the 3GPP LTE standard.[7] While NPSTC looks forward to the eventual inclusion of voice capabilities, it is premature to adopt a requirement into the

[7] Fourth FNPRM at paragraph 29

rules that would mandate public safety broadband networks to be upgraded to include voice.

Additions to the LTE standard are driven primarily by commercial network operators globally. Experience has also shown that not all network operators incorporate all features and functions found within new releases or incorporate them in the exact same manner. New releases contain a plethora of features and functionality allowing network operators to decide how and when new capabilities will be incorporated into their offerings. The public safety network must be allowed to evolve in much the same manner. Every release will contain a variety of features and functionalities, some of which may be beneficial to public safety and some that may not be suitable for widespread deployment or may not be economically feasible for public safety. .

That reality provides public safety the benefit of economies of scale but also the challenge of prioritizing features and approaches pertinent primarily to the public safety market. Until the LTE standard is updated to incorporate voice capabilities <u>and</u> those capabilities are fully tested to ensure they actually meet public safety requirements for mission critical use, there is no operational threshold requirement for a rule mandating that public safety broadband networks be upgraded to support voice. If and when such a rule is adopted in the future, it would need to be predicated on the availability of sufficient funding to execute the requirement. Otherwise, it would simply be an unfunded mandate.

6. <u>IPv4 vs. IPv6</u>

The Fourth FNPRM raises a series of questions concerning the use of IPv4 and/or IPv6. Most of the current applications deployed in public safety are based on IPv4. NPSTC understands that without some translation mechanism or dual-stack implementation, users with IPv4 addresses would not be able to access IPv6 services or communicate with an IPv6 host. Therefore, it would appear to

be too soon to mandate IPv6, especially for the near-term.

NPSTC looks forward to comments on the Commission's more detailed questions regarding IPv4 and IPv6 from technical experts in that area. As in other areas raised by the Fourth FNPRM, NPSTC cautions against adopting detailed technical requirements in this area until the operational impact is well understood and stability in the rollout of the technology to meet public safety requirements is evident.

7. Additional Interfaces

The Commission requests comments on whether it should require public safety broadband networks to adopt the Gxc interface in addition to the interfaces required in the Third Report and Order. Additional industry standards development organization work and waiver region build outs and operation should provide insight into whether there is any public safety operational requirement for this additional interface. NPSTC recommends this not be regulated or required at this time.

8. Network Interconnectivity, Public Safety Roaming and Mobility/Handover

NPSTC's goal is a system that allows any user device to operate anywhere nationwide there is coverage built out, as authorized and prioritized by public safety. Devices would also need to have a basic set of functions deemed critical by public safety. For nationwide interoperability, we believe that some form of nationwide network connectivity is needed, regardless of the architecture. This interconnectivity can be provided by a public safety operated backbone, 3rd party commercial service providers or both. As noted previously in section 3 of these comments, NPSTC believes that one public safety PLMN ID would simplify nationwide interoperability as the only roaming required would be onto commercial networks.

The Commission also raised questions regarding roaming across public safety networks.

NPSTC seeks to minimize the need for public safety roaming while still providing the elements of control and authorization needed for security and proper public safety incident management. Public safety needs a common nationwide architecture that supports these goals. Details and tradeoffs are still being addressed in the public safety community and therefore NPSTC recommends that proscriptive FCC rules on the details of roaming not be required at this time. With a common nationwide architecture, mobility and handover would also be specified during engineering of that architecture and the FCC should not try to regulate mobility and handover at this time.

9. Quality and Priority of Service

The Fourth FNPRM requests comments on quality of service (QoS) and priority access features in release 8 of the LTE standard. Experience shows that the simple two queue priority access as used historically on commercial networks is insufficient for public safety needs. Public safety requires a framework which allows local agencies to specify priority levels for their personnel and to change priority levels of their own and responding mutual aid units for specific emergency events. NPSTC believes the LTE provisions for QoS and prioritization provide a useful framework. However, since these provisions were developed in the standard based on commercial network requirements, it is likely that some additional work will be needed to ensure that there are standardized approaches for priority, with provisions for local agencies to adjust priority levels on an incident requirement basis.

10. Applications

As noted in previous NPSTC comments and the NPSTC Broadband Task Force (BBTF) report, a common set of applications will be needed across the country to enable nationwide interoperability. NPSTC specified five applications in the BBTF Report, i.e., Internet access, VPN

access to any authorized site and to home networks, a status information homepage, provision of network access for users under the Incident Command System and field-based server applications. In its Waiver Order the Commission required support of these 5 applications. Localities, regions or states are also expected to supplement these common applications with applications more specific to their respective jurisdictions.

The key question is whether these common applications should be specified in the Commission rules or in some other manner. As noted previously in these comments, changes to Commission's rules normally entail a multi-year process. Therefore, while NPSTC is gratified the Commission used the BBTF as the requirements for waiver grantees; we are concerned about incorporating a set of common applications in the rules. A mechanism is needed for these applications to be specified without including them in the rules.

11. Interconnection with Public Safety LMR Networks

Today's public safety land mobile radio systems span a number of bands, a mix of analog and digital systems and a variety of capabilities, based on local requirements. Some systems already incorporate IP into the infrastructure deployed and others do not. Some public safety users will want interconnection between their LMR networks and broadband and others may not. Therefore, the advantages/disadvantages, capabilities and costs associated with such interconnections is likely to vary across jurisdictions. While such interconnections can certainly be beneficial, NPSTC does not view such an interconnection requirement as an essential element to the rules needed for broadband interoperability. NPSTC therefore recommends that the decision whether to pursue interconnection remain a local decision based on local operational needs, rather than being proscribed by

Commission rules.

12. Out-of-Band Emissions (OOBE)

The Commission tentatively concludes to adopt the same OOBE limits previously specified in the Waiver Order as part of the rules for the nationwide public safety broadband network. NPSTC supports this tentative conclusion. In particular, there is value in providing stability on basic equipment requirements such as OOBE that impact hardware designs and are essential to help prevent interference.

13. Performance Requirements: Data Rates and Coverage

Cell edge data rates, coverage, number of sites and cost are all linked together on a broadband network. Data rates typically are higher near an eNodeB site and fall off as the user moves further out in a sector away from the site. Therefore the data rates experienced and coverage are both impacted by the number of sites in a system, which in turn of course is impacted by funding. Broadband also typically requires more sites than current narrowband system to provide the same degree of coverage. While public safety entities can generally re-use their established narrowband sites to house and support broadband radio access network (RAN) equipment and LTE antennas, additional sites are needed. These can be sourced by agreements with commercial operators, other antenna site managers or by establishing new sites where necessary.

Each area will face a different combination of factors impacting the availability of sites and therefore the engineering-cost tradeoff for each region can vary. This is particularly true in contrasting the environment in rural areas vs. that in major cities. Major cities normally have a number of building roof tops that can support RAN and broadband antenna sites. Such buildings are generally non-existent in rural areas and the lower density of users and smaller jurisdictional budgets

presents a much different economic model to support the system. Commercial operations which are touted by the Commission for their use of low site architectures routinely deploy high sites in rural areas to provide coverage more economically.

Because of all the complex engineering and economic tradeoffs factors that impact the design of a system will necessarily vary in different regions, NPSTC previously recommended that the Commission leave performance requirements to public safety instead of codifying them into the rules:

> The Commission should trust public safety waiver grantees to deploy systems that they design to match the operability (performance) requirements pertinent to their respective regions and instead, focus on elements that enable interoperability across operable systems. Clearly a system that is not operable cannot be interoperable. However, meeting both operability and interoperability requirements is a multi-faceted challenge impacted by the amount of spectrum available, funding, technology, control and governance. Attempting to mandate performance elements of a system design in the rules would do nothing but establish parameters that may or may not be matched to a given region's needs. Public safety agencies are capable of making decisions on the various tradeoffs that define what is both needed and viable in their respective regions, and should be given the leeway to do so.[8]

NPSTC continues to believe it is preferable to leave these decisions to public safety. However, the Commission has tentatively concluded to require outdoor coverage at minimum data rates of 256 Kbps uplink (UL) and 768 Kbps downlink (DL) for all types of devices, for a single user at the cell edge based on a sector loading of seventy percent throughout the entire network.[9]

In applying these minimum data rates, the Commission tentatively concludes to require each public safety network operator to certify, within thirty days of its date of service availability, that its network is capable of achieving these data rates. The benchmark for "service availability" is defined by the Commission in the Third Report and Order as when the system is being used on a day-to-day

---

[8] NPSTC Comments at pages 9 and 10 submitted July 19, 2010 in response to the Commission's Public Notice DA10-884, released May 18, 2010, at page

[9] Fourth FNPRM at paragraph 61

basis for operational functions by at least fifty users.[10] Under the Commission's tentative conclusion, these certifications would be based on a representation of the actual "as-built" network and accompanied by UL and DL data rate plots that map specific performance levels. The Fourth FNPRM seeks comment on these tentative conclusions, including the appropriate geographic areas for making these measurements and the time frames for compliance. We tentatively conclude that these requirements should be met prior to the date that a network achieves service availability.

NPSTC notes that the data rates proposed are generally consistent with rates being specified in RFPs for major urban areas. However, we are concerned that the specifics of measurement, the application of the rates to systems in both rural and metro areas and the stringent timing of applying these minimum rates essentially from day one of a system operation fails to reflect the reality of system deployments. If the Commission adopts a rule with minimum data rates that cannot be met economically in a rural area, then the rule will have the unintended consequences of preventing any rural deployment whatsoever.

Furthermore, there are jurisdictions, e.g., San Bernardino County, CA, which include both populated cities and significant rural areas with very low population. Even if the Commission were to write a rule that applies the minimum date rates only to metropolitan areas, it is not clear how the rule would be applied in areas like San Bernardino County.

The proposal to apply the minimum data rates almost immediately and required detailed mapping and certification within 30 days does not seem to be compatible with the reality of large system buildouts. In general, deployment of any large communications system for public safety normally proceeds with buildout, preliminary "dry run" testing and optimization, additional testing and optimization based on usage and then expansion to cover the entire area and/or provide

[10] Fourth FNPRM at footnote 32

additional capabilities.

As noted above, NPSTC believes there are very legitimate reasons to leave these requirements to the discretion of public safety. However, if the Commission continues to pursue adoption of a rule for minimum data rates, NPSTC recommends that at minimum, the timing, geographic scope and technical details provide much greater flexibility to reflect the variety of environments and tradeoffs various public safety agencies must incorporate into system planning and deployment. This flexibility should be inherent in any such rule rather than by establishing an inflexible requirement and forcing public safety agencies to incur the additional delays and expense involved in seeking a waiver of the requirement.

The Commission also seeks comment on whether it should impose either a population or geographic bases build out requirement and if so the benchmarks that should be included. In teeing this up for discussion, the Fourth FMPRM raises the possibility of a requirement that each public safety network operator would be required to certify compliance with coverage within 30 days of service availability. While unclear if positioned as a possible additional requirement or as an alternative to the approach above, the Commission also raises questions about a possible benchmarks over a 15 year period, e.g., 40% of coverage within 4 years, 75% coverage within 10 years and 99% coverage within 15 years.

As noted above, NPSTC believes that applying requirements at the point of "service availability" as defined in the Third Report and Order with certifications within 30 days is completely counter to the reality of most public safety system deployments. Therefore, NPSTC opposes such an approach.

NPSTC does understand the Commission's need for some coverage benchmarks to ensure that deployment of a nationwide system proceeds at a reasonable pace. While adopting a phased set of benchmarks over time also appears to be a reasonable approach, a key threshold question is when to start the time clock for any benchmarks adopted.

NPSTC believes it is counterproductive to start the time clock for any coverage benchmarks prior to resolution of the myriad of open issues and the actual start of deployment in a given region. For public safety regions, deployment starts are dependent on a number of factors outside their immediate control. These include 1) the availability of funding still being debated in Congress; 2) governance and rules yet to be decided; 3) the conditions and subsequent additional requirements imposed by the Commission in granting "conditional waivers" which for the most part did not actually result in immediate authorization for deployment; 4) local laws and procedures pertinent to the procurement process; 5) the complexity of the design in a given area; and 6) delays yet to be determined due to any equipment interoperability testing and certification requirements imposed by the Commission.

Given the above, NPSTC recommends that the Commission not rush to impose coverage requirements in the rules in the absence of resolving the many open issues and determining through experience how those resolutions impact actual deployment. Once the many open issues are resolved and the real impact known, the necessity and specifics of applying some set of phased coverage benchmarks can be better understood and determined. NPSTC also notes that the most appropriate coverage priorities in a given region are best determined by or in consultation with public safety representatives who have firsthand knowledge of the particular regions' needs.

14. Additional Performance Issues

NPSTC recommends that network capacity, robustness and hardening, security and encryption all be deferred to public safety decision-making after key decisions are made on the approach for the overall system architecture. The specific parameters and steps required ensuring comparable levels of system robustness and hardening will inherently vary by region. Some regions are more prone to hurricanes and tropical storms, while others are more prone to earthquakes, etc. Therefore, robustness and hardening are operational cost/benefit issues for which public safety needs and solutions will vary significantly throughout the nation. The local agencies in a given region know through experience what level of robustness and hardening is required and how best to achieve that level given the environment in the region and the funds ultimately available.

While there is validity in deciding provisions for security and encryption to ensure nationwide interoperability, some provisions need to be made to allow security and encryption at the operational level to be modified and upgraded over time if appropriate. Security, at all levels is inherently important to public safety agencies so system planning and engineering will incorporate necessary security features that probably will change over time. In addition, use of the network by Federal agencies may impact the specific encryption provisions required. NPSTC looks forward to comments from technical experts in these areas.

15. Interference Coordination

NPSTC agrees that preventing interference among adjacent system deployments is important. Therefore NPSTC has supported generic requirements the Commission imposed in its Waiver Order that require waiver grantees in adjacent areas to coordinate with one another to minimize any interference problems. NPSTC understands that the physical layer of LTE is designed to continue operation in the presence of some levels of interference.

While NPSTC believes the requirement to coordinate to prevent interference is important, the specific steps needed should be left to public safety to decide. We note that the scope of such coordination may also be dependent on the architecture decisions ultimately made and how regional deployments fit within an overall nationwide architecture. In any case, interference prevention is part of the normal planning and engineering of a system. Therefore, NPSTC understands requiring such coordination by adjacent regions, but does not believe the planning and engineering needs to be specified in great detail in the rules.

16. Eligibility for Use of the Broadband Network

As NPSTC and its member organizations have discussed the potential for broadband with public safety agency representatives, a number of issues have arisen concerning eligibility for use of the public safety broadband network. These include the potential to accommodate Federal users, local and state users outside strict police, fire and emergency medical boundaries and critical infrastructure industry (CII) users, e.g., utilities. These issues arise primarily as part of the nationwide public safety (local, tribal, state, and Federal) interoperability vision for the broadband network and also in the context of partnering with Federal, military bases and/or CII users to deploy the system in certain areas.

NPSTC supports a process to allow Federal agencies as eligible users on the broadband network, but there needs to be a standardized nationwide process established and managed by the PSBL rather than dozens or hundreds of local agreements. NPSTC recommends this type of governance approach as it will help improve interoperability across local, tribal, state and Federal levels of government as needed to promote public safety. In particular, some partnerships with federal installations could also help ensure coverage continues from a local jurisdiction into the area to enhance the safety and security of public safety, military or other Federal personnel, as well as the

general public that public safety is charged to protect and serve.

NPSTC also recommends the Commission clarify that all types of government employees, not just core Fire, Police, and EMS users, can use the network, as long as the core users have control over priority access to the network. Given that interoperability is a foundational goal of the nationwide public safety broadband network, it is counterproductive for the FCC to proscriptively limit which government users can have access to the broadband network In any given situation, police, fire and EMS, transportation, road crews, etc. could need to share information on various databases, or, video from various sources. Preventing government users other than police, fire and EMS from using the network on a regular basis also means that they would not be trained on the equipment which could hamper expeditious operation in an emergency.

In addition, use by Critical Infrastructure Industries is appropriate where public safety agencies agree to that use and manage its prioritization. For example, in any given incident, public safety may very well have an urgent priority to communicate with the power company and/or the gas company to turn off utilities as part of the effort to save lives. In such an instance, the principal purpose of this communications is clearly to support of public safety and should qualify as eligible under Section 337 as long as public safety is in control of the prioritization.

NPSTC also notes that the issues of Federal use, operations by local/state agencies outside of police, fire and EMS and Section 337 eligibility for non-government organizations were addressed extensively in previous rulemakings regarding the 700 MHz Narrowband spectrum.[11] Since both the broadband and narrowband 700 MHz bands are subject to Section 337, NPSTC believes that those previous decisions may also help provide the legal basis for decisions going forward on the

[11] See First Report and Order in WT Docket 96-86,released September 29, 1998 and Second Memorandum, Opinion and Order in WT Docket 96-86, released August 1, 2000.

broadband spectrum, with appropriate modifications to reflect that the broadband spectrum is licensed nationwide to the PSBL instead of individual local or state agencies as in the Narrowband spectrum.

17. Use of the 4.9 GHz Band and Backhaul Spectrum

NPSTC is on record in docket 07-100 that better coordination methods are needed for the 4.9 GHz band. Today backhaul is a prime use of the 4.9 GHz band and more efficient use is needed. One way is to specify a maximum ERP and a larger antenna gain thus reducing beam width. The FCC should explore using better coordination and larger antennas to make more efficient use of the 4.9 GHz band for broadband backhaul.

Backhaul will be a significant issue for both public safety and commercial operations at 700 MHz. The Part 101 fixed microwave spectrum is shared and crowded. Suburban and rural areas where fiber connections are difficult and expensive to deploy need the most attention. A separate proceeding is needed to identify additional resources and NPSTC recommends that this be addressed in a separate NPRM to provide the proper focus on this issue.

18. Conformance Testing

Commercial operators have developed standards and requirements for their authorized devices. These operators require conformance testing to ensure that devices operate properly on their network. Similarly, public safety will require some mechanism for conformance testing of devices it deploys. A common nationwide architecture that NPSTC has proposed may allow this testing to be done in ways that reduce cost and duplication. However, the details would need to be addressed after decisions are made on the larger issues of architecture and governance. Until that is done, NPSTC believes it is premature for the Commission to try and regulate conformance testing.

Summary

NPSTC congratulates the Commission on issuing such a comprehensive Fourth Further Notice of Proposed Rulemaking. As addressed in the comments herein, NPSTC supports a nationwide architecture with provisions for regional control, together with rules essential to nationwide interoperability. While NPSTC believes all the questions and proposals contained in the Fourth FNPRM are extremely important, the key question is what rules are essential to nationwide interoperability. NPSTC views the answer to that question to be dependent on what architecture and governance is decided for public safety broadband. NPSTC also cautions against codifying too many detailed rules at this early stage of broadband deployment. Given the many detailed rules proposed, it is likely that a number of the rules would need to be modified based on additional deployment and operational experience yet to come. The multi-year process to do so could further delay the provision of broadband service to public safety.

Respectfully submitted,

Ralph A. Haller, Chair
National Public Safety Telecommunications Council
8191 Southpark Lane, Number 205
Littleton, Colorado 80120-4641
866-807-4755

April 11, 2011