Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 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
	)	
	)	
Amendment of Part 90 of the Commission's Rules	)	WP Docket No. 07-100
	)	

COMMENTS OF THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Lawrence E. Strickling
Assistant Secretary for Communications and Information

Kathy D. Smith
Chief Counsel

Anna M. Gomez
Deputy Assistant Secretary for Communications and Information

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4713
Washington, DC 20230
(202) 482-1850

June 10, 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Telecommunications and Information Administration (NTIA) commends the Federal Communications Commission for conscientiously addressing our first responders' communications needs, and continuing to make these needs a priority. Proceeding from the shared vision of an efficient and effective nationwide interoperable public safety wireless broadband network and recognizing this rare opportunity to help realize that vision in the near future, the Administration, in these Comments, highlights important issues in the development of an overarching framework to achieve this common vision and suggests an appropriate course of action.

The Administration supports legislation to create a not-for profit Public Safety Broadband Corporation ("Corporation") that would effectively oversee a nationwide network operation tailored to meet the needs of the local, State, Tribal, and Federal public safety communities. The Corporation would consult and coordinate with relevant public safety officials at State, local, or Tribal jurisdictions, as well as Federal entities where appropriate, on matters within their purview. This corporate structure would be the most efficient and cost-effective way to ensure the deployment of a truly nationwide, interoperable public safety network.

These Comments address the technical issues presented in this rulemaking through the prism of such a nationwide public safety corporate structure. Specifically,

- Intra-public safety network roaming ceases to be a concern in a nationwide network, but remains a significant problem and cause of inefficiencies in a series of regional networks. The Corporation should require only a single Public Land Mobile Network (PLMN) identifier for the purpose of facilitating roaming among public safety users of a single nationwide public safety broadband network and commercial networks;

- The Corporation should develop a nationwide prioritization and Quality of Service framework that is consistent with State, local, Tribal and Federal user expectations;

- The Corporation should bear primary responsibility for assessing the need for required applications or services, in coordination with State, local, Tribal and Federal jurisdictions; and

- The Corporation should develop device requirements that take into account costs of additional, public-safety-only functionality, interoperability with legacy LMR networks, 2G/3G/4G commercial wireless network roaming capability, and non-LTE technology support such as WiFi and Bluetooth.

The Commission's role in facilitating a nationwide interoperable public safety broadband network remains critical. Most importantly,

- The Commission should retain its traditional and essential role in regulating the Corporation as a wireless licensee, including requiring interference coordination between the Corporation and adjacent commercial networks;

- The Commission should require the Corporation to certify interoperability and conformance testing as applicable to infrastructure and devices;

- The Commission should require certain security and encryption features needed by Federal users;

- The Commission should promote standards-based technologies as a foundation and framework for achieving interoperability;

- The Commission should permit and enforce fixed use of the public safety broadband spectrum only on an ancillary basis; and

- The Commission should help facilitate deployment in the period leading up to the establishment of the Corporation by taking a leading role in the ongoing gathering and assessment of data on public safety broadband requirements, applications and features.

Federal entities are important partners in State, local, Tribal, and regional emergency and public safety response. The Commission has wisely determined to preserve the existing principle of Federal eligibility to use the public safety broadband network, subject to license holder approval. Federal agency administration and procurement of assets are centralized. The

Corporation would provide an efficient single point of contact for making service arrangements on the public safety broadband network. These service arrangements should permit Federal entities flexibility to choose from a variety of service options.

The Commission also should acknowledge the critical role that public safety support services, such as nuclear and power plant relief and recovery personnel, transportation agencies, and road crews, often play in emergency response. As long as the use of the 700 MHz band is consistent with the statutory purpose of Section 337, to protect the safety of life, health, or property, the Commission should permit the Corporation, in consultation with local, State, Federal and Tribal jurisdictions, to offer service to public safety support providers. Such use would be subject, in a particular emergency, to the decisions of the incident commander.

Before the

Federal Communications Commission
Washington, DC 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
	)	
	)	
Amendment of Part 90 of the Commission's Rules	)	WP Docket No. 07-100
	)	

COMMENTS OF THE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

As the President's principal adviser on telecommunications policies, the National Telecommunications and Information Administration (NTIA) submits these comments on behalf of the Executive Branch.[1] The Federal Communications Commission deserves congratulations for its diligent efforts to address the communications needs of our nation's first responders, and

[1] NTIA is the Executive Branch agency principally responsible for the development of telecommunications policies pertaining to the Nation's economic and technological advancement and to the regulation of the telecommunications industry, for the coordination of the telecommunications activities of the Executive Branch, and for the effective presentation of the views of the Executive Branch to the Commission. *See* 47 U.S.C. § 902 (b) (2). In formulating these comments, NTIA also incorporated input from the Interdepartment Radio Advisory Committee (IRAC), the Emergency Communications Preparedness Center (ECPC), and other Executive Branch entities. The IRAC, composed of 19 member agencies, assists in the assignment of radio frequencies to the Federal government and in the formulation of spectrum management policies for the Executive Branch. The ECPC, composed of representatives from 14 Federal agencies, is the Federal interagency focal point for interoperable and operable communications coordination.

for making public safety communications a priority.[2] The Administration's goal is to achieve the most efficient and effective nationwide interoperable public safety wireless broadband network possible. With a rare opportunity to help realize this objective in the near future, NTIA urges the Commission to be extremely mindful of the criticality of an overarching nationwide framework to a viable public safety broadband network. These Comments highlight important issues in the development of such a framework and suggest an appropriate course of action.

INTRODUCTION

The nation needs a public safety broadband network that is cost-effective, state-of-the-art, nationwide, and interoperable, and that rests on a stable, competent, and financially viable governance structure. To succeed, this network must accomplish a number of objectives. Specifically, the network must: (1) deliver broadband communications meeting appropriate public-safety-grade levels of service that are reliable and secure; (2) enlist the trust of public safety agencies that will migrate traffic to this new network; (3) enable seamless communications between public safety agencies and jurisdictions, as well as Federal responders; (4) provide a platform for a wide range of affordable equipment and applications; and (5) leverage commercial platforms and technologies that can evolve to take advantage of innovation on a cost-effective basis.

To facilitate effective nationwide governance and efficient use, the Administration supports legislation to create a not-for-profit corporation which, for purposes of these Comments,

[2] Service Rules for the 698-746, 747-762 and 777-792 MHz Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band; Amendment of Part 90 of the Commission's Rules, *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, FCC 11-6, 76 Fed. Reg. 10295 (2011) (hereinafter *Order/FNPRM*).

is referred to as the "Public Safety Broadband Corporation" (the Corporation).[3] The Administration proposes that the Corporation be governed by a Board of Directors that would be able to effectively oversee a nationwide network operation tailored to meet the needs of the State, local, Tribal, and Federal public safety communities. This corporate structure would be the most efficient and cost-effective way to ensure the deployment of a truly nationwide, interoperable public safety network.

The new Corporation would manage network development and construction by contract(s), thereby increasing the likelihood of a coordinated and interoperable network.[4] To ensure public safety community involvement, the Administration also proposes to make planning grants available to State, local, and Tribal jurisdictions to assist in developing the most effective and efficient local deployment and to maximize use of existing facilities where possible. The Administration has incorporated funds for the deployment of the network with such a governance structure into President Obama's Fiscal Year 2012 Budget.[5]

More specifically, the Corporation, with the assistance of professional staff and contract support as necessary, would perform the following functions:

- hold the spectrum license;

[3] The creation of such a Corporation requires Congressional action. The Administration stands ready to support such authorizing legislation.

[4] The Corporation should decide the number of contracts (ranging from one to several) to be bid for construction and operation of the network.

[5] The President's "Wireless Innovation and Infrastructure Initiative" would allocate, from the proceeds of voluntary incentive auctions, nearly $7 billion for the construction of an interoperable public safety broadband network; $5 billion for broadband infrastructure in rural areas, which will facilitate public safety deployment in those hard-to-serve regions; and $3 billion for wireless research and development, which will include a significant number of public safety broadband technical and operational issues. "President Obama Details Plan to Win the Future Through Expanded Wireless Access" (Feb. 10, 2011) *available at* http://www.whitehouse.gov/the-press-office/2011/02/10/president-obama-details-plan-win-future-through-expanded-wireless-access.

- set policies for network requirements, standards, management, and operations;
- coordinate public safety representation before standards-setting and testing bodies; and
- oversee, through contract(s) where appropriate, the operation and functioning of the network, thereby ensuring that the system is maintained and refreshed or upgraded on a nationwide basis.

The Corporation would also consult and coordinate with relevant public safety officials in State, local, or Tribal jurisdictions, as well as with Federal entities, where appropriate, on matters within their purview. As public safety experts in their respective jurisdictions, these officials provide valuable insight and knowledge and must serve key roles in the deployment of a nationwide system. Within the context of an established nationwide public safety network, State, local, and Tribal officials would enable and recommend appropriate locations for local infrastructure deployment, evaluate the adequacy of requirements for disaster-resistant equipment, select and manage certain applications for their respective jurisdictions, and potentially assign priorities to incident responders and their applications, per nationwide frameworks.[6]

The alternative to this model, which would rely on a "network of networks" or network of independently operated networks, is not efficient and is not likely to be sustainable, if it is even built.[7] This alternate approach would likely lead to higher costs and an inability to solve

[6] The Incident Command System (ICS) is a standardized, on-scene, all-hazards incident management approach that enables a coordinated response among various jurisdictions and functional agencies, both public and private. The incident commander oversees and sets priorities among incident response teams and the communications assets that these teams use. *See generally*, Federal Emergency Management Agency, "Incident Command System (ICS)," *available at* http://www.fema.gov/emergency/nims/IncidentCommandSystem.shtm.

[7] *Order/FNPRM*, ¶ 18.

technical issues that threaten the goal of true nationwide interoperability similar to the situation faced by legacy public safety voice networks today. The better course of action is to enable simplified, inherently interoperable communications on the new public safety broadband network. The most direct way to do this is to create an expert, responsible, nationwide operator to oversee the build-out of a single nationwide public safety network that leverages commercial platforms to the maximum extent practical.

The Commission should adopt minimal rules now. Instead of creating a rigorous regulatory framework, the Commission should empower a public safety broadband operator to deploy with the flexibility necessary to keep pace with cutting-edge technology. To this end, and as discussed further below, the Commission should set the stage to permit the Corporation to take responsibility for the key technical decisions appropriate to a wireless licensee. However, the Commission should retain its traditional regulatory and enforcement powers over the Corporation, as it would over every other licensee. In addition, the Commission should promote the adoption of standards-based technologies as a foundation for such interoperability and should not permit proprietary technology that hinders nationwide interoperability. The Commission should also require that the Corporation ensure that all devices and equipment undergo adequate conformance and interoperability testing and mandate certain security and encryption features required by Federal missions. The Commission should permit fixed uses of the public safety broadband spectrum only on an ancillary basis, ensuring that there will be adequate mobile capacity in emergency situations. The Commission should also avoid or mitigate potential implementation risks by taking a leading role in the ongoing assessment of public safety broadband requirements, applications, and features; the use of open, as opposed to proprietary, technologies; and the availability of accredited testing laboratories. The Commission should use

this assessment to gain a better understanding of how best to cultivate an interoperable public safety broadband network meeting the objectives identified above.

I. THIRD REPORT AND ORDER

The Commission's designation of a nationwide system standard for public safety broadband will help launch a new broadband era in public safety communications.[8] The selection of Third Generation Partnership Project (3GPP), Long Term Evolution (LTE) as the country's standard helps ensure that emergency and public safety responders can communicate regardless whether the response is in their own localities or anywhere else in the country. A uniform standard also promotes economies of scale in procuring equipment and services.

To chart a successful course, however, the new public safety broadband network requires a governing body with the decision-making authority to deploy, manage, operate, and maintain the nationwide network. The nationwide public safety broadband network needs -- and public safety and emergency responders and their communities deserve -- interoperability, effectiveness, and efficiency. The Commission, working with the Emergency Response Interoperability Center (ERIC) and Federal agencies with relevant missions and equities, such as the Departments of Commerce (Commerce), Homeland Security (DHS), and Justice (DOJ), can help facilitate a smooth transition from the current licensee to a public safety corporation with the authority and resources to operate a nationwide network.

[8] *See, e.g.*, 3GPP Standard, Evolved Universal Terrestrial Radio Access ("E-Utra"), Release 8 ("LTE"), and associated Evolved Packet Core ("EPC") [hereinafter "LTE Release 8"], *available at* http://www.3gpp.org/Release-8. 3GPP, "Third Generation Partnership Project," is a collaboration of telecommunications associations dedicated to the formulation, maintenance, and development of technical standards and reports for the Global System for Mobile Communication (GSM), including evolved radio access technologies and enhanced data rates for GSM Evolution. Issues relating to backward compatibility are addressed *infra* note16.

II. FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING

Public safety broadband service must be both operable and interoperable.[9] Nearly ten years after 9/11, this goal still eludes public safety communications.[10] Today, a number of factors are coming together to make this goal achievable. Public safety holds unused spectrum designated for broadband in the valuable 700 MHz radio frequency band. The Commission has designated LTE as the new technical standard for public safety broadband. The Administration has awarded seven early deploying jurisdictions $382,467,000 in Broadband Technology Opportunities Program (BTOP) infrastructure grants for public safety projects, created a demonstration program to test public safety applications of LTE broadband, and proposed a Fiscal Year 2012 Budget that includes funding for this initiative.[11] In this proceeding, the Commission has a unique chance to help shape the future of public safety broadband communications to avoid the interoperability problems that plague legacy voice systems today. The Commission must stay true to the overarching goal of an operable and interoperable nationwide public safety broadband network.

---

[9] The meaning of "interoperability" is discussed in the next section, Section II.A., *infra*.

[10] Letter from Hon. Julius Genachowski, Chairman of the Federal Communications Commission to Hon. Henry Waxman, Chairman, House Committee on Energy and Commerce (July 20, 2010), Attachment at 2-3, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-300681A1.pdf.

[11] Broadband USA: Connecting America's Communities, "Grants Awarded: Broadband Infrastructure Projects,"*available at* http://www2.ntia.doc.gov/infrastructure (BTOP infrastructure grants). Within Commerce, NIST and NTIA have partnered to create the Public Safety Communications Research (PSCR) program, which is funded by DHS and DOJ. The PSCR Program is participating in LTE standards development and is in the process of building a demonstration LTE network for public safety testing purposes in Boulder, Colorado. *See generally*, "Public Safety Research Program," http://www.pscr.gov/. The President's budgetary proposal is discussed *supra* note 5.

A. Harmonized Definition of "Interoperability"

In formulating a definition of interoperability, the Commission should, as it suggests, seek to harmonize terminology with that of other interested Federal agencies.[12] The DHS SAFECOM program defines communications interoperability as "the ability of emergency response agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, when authorized."[13] To avoid confusion, the Commission should use terminology consistent with this definition, which aims to "ensur[e] that the public safety community, whoever and wherever they are, is able to communicate with one another," using voice as well as broadband data communications.[14] Use of a consistent lexicon will simplify discussions over standards, compliance, and related matters, and facilitate the coordination of Federal programs and regulations affecting public safety communications.

B. Nationwide Network Architecture

1. Technical Compatibility and Evolution

The *Order/FNPRM* tentatively concludes that the Commission should adopt architectural guiding principles consistent with a public safety network composed of a set of "interoperable, regional or tribal all-IP networks operating in the public safety broadband spectrum."[15] The Administration believes that this approach is not the best way to achieve the goal of a single, nationwide, interoperable network.

---

[12] *Order/FNPRM*, ¶16.

[13] SAFECOM "Frequently Asked Questions," *available at* http://www.safecomprogram.gov/SAFECOM/about/faq/#1126.

[14] *Order/FNPRM*, ¶ 16.

[15] *Order/FNPRM*, ¶18.

The nationwide public safety broadband network will have to integrate those who deploy early and have the ability to update the network for new software releases and other technological advances. The most effective way to do so is to have the Corporation oversee the system's construction and operation, including network management, user requirements, participation in standards development, provisioning, upgrades, procurement, and technical compliance. This Corporation would have the perspective, speed, and flexibility to stay abreast of new technology and to adapt to evolving user needs.[16] For instance, the Corporation could decide which features to support, and perform full interoperability and conformance testing on every interface for all network software upgrades.[17] Further, reducing the number of different network configurations simplifies interoperability testing of new features and releases. By contrast, a network of networks would have to regression test each software release (biannually or even more frequently) against every other network configuration, over-complicating nationwide harmonization and jeopardizing interoperability.

Accepting the premise of a nationwide operator narrows the architectural and technical issues that the Commission must address. Unlike a patchwork quilt approach, a single nationwide network eliminates the need for roaming when a public safety user travels from one public safety jurisdiction to another.[18] Similarly, a single nationwide network would not require

[16] *Order/FNPRM*, ¶¶ 17, 25-26. For this reason, the Commission should not attempt to mandate specific upgrades or interfaces, but instead make the Corporation responsible for evolving the system. The Commission should also reconsider its decision to require backward compatibility, again leaving the decision to the network operator. *Id.* at ¶¶ 11,24,29. The Commission could retain adequate oversight by imposing reporting requirements on the Corporation. *Order/FNPRM*, at ¶ 118.

[17] Interoperability testing ensures that different hardware or software can work together harmoniously, while conformance testing ensures that a given product in fact meets specifications. *See infra* Section II.C.5.

[18] *See infra* Section II.C.1; note 32. *See generally*, GSMA PRD IR.88 "LTE Roaming Guidelines: 3.1" (Feb. 17, 2011), *available at* http://www.gsmworld.com/documents/IR8831.PDF. Public safety organizations have recognized the value of a nationwide network architecture. *See, e.g.*, "NPSTC

a clearinghouse or roaming hub to provide connectivity among disparate public safety regions or networks.[19] The Corporation could, however, leverage other pieces of existing commercial networks, including infrastructure, billing systems, call centers, and roaming subsystems, without putting at risk nationwide interoperability.[20]

2. Economies of Scale

A single nationwide operation is also more cost effective, as it would reduce or eliminate unnecessary duplication of key elements of the Evolved Packet Core (EPC). In a series of networks, each network would require deployment of all EPC elements. Under a nationwide architecture, however, the Home Subscriber Server (HSS) and Policy Control Resource Function (PCRF) are elements of the EPC capable of serving the entire network. This would allow for a planned distribution of other EPC elements, Serving Gateways (SGW), Packet Gateways (PGW), and Mobility Management Entities (MME), which could be deployed regionally to make the most cost-effective use of network resources.[21] Such geographic dispersal facilitates the build-out of denser networks and would permit those jurisdictions deploying early to focus their

---

Presents Strong Case for a Nationwide Broadband Concept for Public Safety" (Mar. 10, 2011), *available at* http://www.npstc.org/pressRelease.jsp.

[19] A nationwide network would allow use of a clearinghouse or roaming hub for roaming on commercial systems. The Commission plans to address roaming onto commercial systems separately. *Order/FNPRM*, ¶ 36 & n.97.

[20] Indeed, commercial carriers or system integrators may have a key role in helping to build and/or operate a public safety broadband network. The new Corporation should be able to forge agreements that leverage commercial infrastructure to facilitate deployment or operability. Such commercial relationships can help the Corporation stay current with technology advances.

[21] The EPC is a group of elements and functions that may be distributed geographically. The EPC is the IP backbone of the LTE system, and handles overall control functions. It contains a number of elements: the MME, which controls the mobility of the UE's (user equipment devices) and tracks mobiles and associated data cards as they move through the network; the SGW/PGWs, which function like large routers that direct all IP traffic in the system; the PCRF, which controls Quality of Service and policy enforcement; and the HSS, a subscriber database used to authenticate subscribers and devices.

resources on Radio Access Network (RAN) build-out.[22] Subscriber databases located in the HSS can be centrally housed and replicated as necessary for redundancy. Finally, a single nationwide network allows fewer external interfaces than a network of networks approach, thus offering better network security.

By contrast, a patchwork quilt approach would require each independent network to deploy its own HSS and PCRF, thereby driving up costs overall. A single nationwide network could also take advantage of the larger user base and territory to negotiate cost-effective master contracts for user devices and network infrastructure, and to leverage existing commercial infrastructure for collocation purposes, possibly as part of such master agreements. Regional operators would not have the same power in bargaining with commercial vendors, thus increasing costs for public safety.

3. The Role of State, Local, and Tribal Jurisdictions

Notwithstanding the need for a nationwide public safety broadband architecture, certain aspects of the network such as capacity, coverage, cell site placement, hardening, certain aspects of reliability, and backhaul provisioning are inherently local in nature.[23] They vary according to terrain, demography, and other characteristics, making a one-size-fits-all approach inappropriate.[24] The Commission should refrain from imposing uniform requirements given

[22] The RAN is that portion of the LTE network connecting the UEs and EPCs. The eNodeBs, or the LTE equivalent of cellular base stations, and backhaul connections connecting the eNodeBs to the core are the main components of the RAN.

[23] "Hardening" generally refers to actions taken to make a network infrastructure able to withstand disasters, including by means of strengthened towers and additional back-up generating capacity for cell sites. While survivability modeling might prove useful to mitigate risks associated with possible incidents, the Corporation, in consultation with the relevant jurisdictions, should bear ultimate responsibility for such planning efforts. *See also* Reliability and Continuity of Communications Networks, Including Broadband Technologies, *Notice of Inquiry*, FCC 11-55, PS Docket No. 11-60 (rel. Apr. 7, 2011).

[24] *Order/FNPRM*, ¶¶ 63-64, 70.

such innately local characteristics. Rather, the Commission should defer to the Corporation, which would consult with the relevant State, local, or Tribal jurisdictions regarding these matters, and Federal entities as appropriate, and incorporate their input into its deployment plans.[25]

C. The Role of the Corporation in Technical and Network Decisions

In this proceeding, the Commission should adopt only those rules that are essential to ensuring the efficient and effective use of the 700 MHz public safety spectrum, and leave to the Corporation the flexibility to make decisions to further innovation and facilitate the nimble, day-to-day functioning of the network. A single nationwide network will simplify and inherently harmonize technical operations. An empowered Corporation would have the competence, perspective, and resources needed to swiftly address many of the issues raised in the Commission's public safety proceedings.

1. Roaming

The extensive discussion the *Order/FNPRM* devotes to public safety/public safety roaming and how to manage it illustrates the complications inherent in a series-of-networks approach.[26] More specifically, Public Land Mobile Network (PLMN) identifiers facilitate roaming among different networks by classifying network and user equipment as "visitor" or

[25] It is important that Tribal law enforcement agencies, Tribal emergency management agencies, and other first responders that serve Tribal communities be provided adequate notice and a meaningful opportunity to comment on this Notice of Proposed Rulemaking. The Federal government has a trust responsibility to assist Tribal governments in their efforts to improve public safety in Indian Country. Improving public safety communications is critical to those efforts. The Administration encourages the Commission to reach out and consult with Federally-recognized tribes, in order to provide them an opportunity to articulate their views and the real world impact this proceeding may have in Tribal communities. *See e.g.*, "Consultation and Coordination with Indian Tribal Governments," Executive Order 13175, § 8 (2000) (independent agencies encouraged to comply with the directive).

[26] *Order/FNPRM*, ¶¶ 35-37, 85-89, 93-99.

"home," *i.e.*, roaming or not.[27] As the Commission notes, the numbers available for PLMN identifiers are finite and used worldwide by 3GPP wireless providers.[28] PLMN identifiers proliferate with regional networks, as suggested by the *Order/FNPRM*, increasing the complexity of roaming administration.[29] With regional networks and their associated PLMN identifiers, public safety/public safety roaming would require corresponding use of roaming hubs or clearinghouses, with associated costs and technical issues, for each region. Moreover, each region would have to invoke similar processes and incur similar costs for public safety/commercial roaming. The *Order/FNPRM* asks numerous questions about how roaming under the "network of networks" approach should work, including how to facilitate public safety/public safety roaming agreements, how to authenticate visitors, and how to handle charges.[30]

The Administration proposal vastly simplifies the issue because the Corporation would only need a single PLMN identifier and would have no need for roaming within the public safety broadband network.[31] Thus, a nationwide architecture would avoid the public safety/public safety roaming complications caused by a regional networks approach.[32] A nationwide network

---

[27] PLMN identifiers are also known as Home Network Identifiers (HNIs). They comprise a mobile country code (MCC) and a mobile network code (MNC).

[28] *Order/FNPRM*, ¶ 32.

[29] *Order/FNPRM*, ¶¶ 32-33.

[30] *See, e.g., Order/FNPRM*, ¶¶ 35-37, 85-89, 93-99.

[31] Commercial carriers in the United States typically only have one PLMN identifier. *See, e.g.*, Remarks of Brian Daly, Director, Core Network & Government/Regulatory Standards, ATT, "FCC Interoperability Forum" (Mar. 4, 2011), *video available at* http://reboot.fcc.gov/video-archives/?utm_source=fcc.gov&utm_medium=rotator&utm_campaign=live-archive.

[32] A single operator using a single PLMN identifier would not need a roaming hub or clearinghouse and associated business and technical processes to enable visiting public safety users to use a host public safety network, as visitor and host would all be part of a single nationwide public safety broadband

would use the PLMN identifier only for roaming between the public safety broadband network and commercial networks.[33] The Corporation would also be in the best position to decide the optimal technical method for handing over messages between eNodeBs within the network itself.

Also, a regional networks approach inflates the cost of the network. For example, the EPC houses the network elements that track roamers.[34] This patchwork quilt would increase the number of EPC elements and associated infrastructure costs required to implement this approach. The series of networks approach thus creates a number of operability and interoperability issues. For example, there are technical limitations on the number of simultaneous PLMNs that an eNodeB can transmit. There is also a limit on the number of PLMNs that can be programmed on the Universal Subscriber Identity Module (USIM) that would allow a user access to a given network.[35] In addition, a series of networks approach would require creating regional network number schemes, and associated number administration and interoperability complications. Public safety/public safety roaming should not be used to track and properly treat users throughout the network when there are other, better approaches, *e.g.*, specific mapping of

---

network. Thus, the issues raised in the *Order/FNPRM*, ¶¶ 35-37, 85-89, 93-99, do not arise. The *Order/FNPRM*, ¶ 33 mistakenly states that the PSCR program supports a "hybrid" approach to the assignment of PLMN identifiers.

[33] The Alliance for Telecommunications Industry Solutions (ATIS) International Mobile Subscriber Identity (IMSI) Oversight Council (IOC) oversees the management of PLMN identifiers. The Corporation should obtain the PLMN identifier from ATIS IOC. If necessary, the Corporation should authorize appropriate standards body experts to perform this task. ATIS recently eliminated the need for membership in the GSM Association (GSMA) in order to obtain this number. "International Mobile Subscriber Identity (IMSI) Assignment and Management Guidelines and Procedures," § 6.0 (Dec. 2010), *available at* http://www.atis.org/IOC/Docs/Guidelines/IMSI-Guidelines-v12.doc. The GSM Association (GSMA) has released a preliminary version of LTE roaming requirements. GSMA PRD IR.88 "Roaming Guidelines: 3.1" (Feb. 17, 2011), *available at* http://www.gsmworld.com/documents/IR8831.PDF.

[34] *See supra* note 21.

[35] The USIM identifies the subscriber using a mobile device.

International Mobile Subscriber Identifiers (IMSIs), Tracking Area Identifiers (TAIs), and potential use of next-generation phone numbers.[36]

The Corporation will have to confer with State, local, Tribal and Federal jurisdictions on how to deploy each portion of the Radio Access Network (RAN).[37] Together, they would assess how user needs vary among jurisdictions, and what over-engineering is needed to accommodate public safety users from outside the jurisdiction.[38] In contrast to a regional networks approach, with a nationwide operation, intra-system public safety/public safety roaming raises only planning, design, and resource issues, rather than additional technical roaming and administrative concerns. Although a nationwide architecture would still require agreements to facilitate roaming with commercial carriers, the Corporation could efficiently negotiate agreements on behalf of the entire public safety broadband network. [39]

---

[36] It is likely that public safety users will use a next-generation phone number, a combination of phone number and e-mail address, or "ENUM," for their 700 MHz broadband communications. Per ITU-T Recommendation E.164 Number Mapping (ENUM), ENUM maps telephone numbers to IP addresses that can be used in Internet communications. International Telecommunications Union, "ENUM," *available at* http://www.itu.int/osg/spu/enum/. A study item associated with the LTE Demonstration Network at the PSCR program is currently investigating the question of what addresses should be assigned to public safety broadband users. *See generally, supra* note 11.

[37] The RAN is that portion of the network between the user equipment and the EPC that includes the eNodeBs.

[38] In addition, the operator will need to determine how best to effectuate interconnection among areas of the network that are geographically separated. *Order/FNPRM*, ¶¶ 38-42.

[39] The Commission states that it will address public safety/commercial roaming separately. *Order/FNPRM*, ¶ 36 & n. 97. There, the Commission should also address whether and how prioritization features such as Wireless Priority Service, Government Emergency Telephone Service, and NGN Priority Service, which apply to communications by key leadership on existing commercial networks, will be available on commercial broadband networks. *See generally*, "Wireless Priority Service," *available at* http://wps.ncs.gov/; "ITU-T's Definition of NGN," *available at* http://www.itu.int/en/ITU-T/gsi/ngn/Pages/definition.aspx. Moreover, the Commission should address the implications of its recent data roaming order for the public safety broadband network. Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers and Other Providers of Mobile Data Services, *Second Report and Order*, WT Docket No. 05-265, FCC 11-52 (rel. Apr. 7, 2011), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0408/FCC-11-52A1.pdf.

2. Prioritization and Quality of Service

The Commission asks how the public safety broadband network should support prioritization and Quality of Service (QoS), whether there should be a national prioritization scheme, and how this would function in the public safety/public safety roaming context required under a "network of networks" approach.[40] A single nationwide architecture answers these questions by establishing a single a nationwide prioritization and QoS scheme that is always in effect. Consistent priority indicators and procedures, as well as consistent QoS expectations, will allow State, local, Tribal, and Federal public safety agencies to respond swiftly and effectively to emergencies both within and outside their respective jurisdictions.[41] Through the Corporation's coordination with State, local, Tribal, and Federal entities, priority and QoS mechanisms would permit these jurisdictions appropriate flexibility to respond to individual emergencies and other changing circumstances.[42]

---

[40] Prioritization refers to determining which users have precedence in connecting to the network, while QoS refers to maintaining performance for a given application within an acceptable range, once a connection is established. *Order/FNPRM*, ¶¶ 46; 90-92.

[41] The Government Emergency Telecommunications Service (GETS) is a White House-directed emergency telephone service for use by Federal, State, local, and Tribal government, industry, and non-governmental organization (NGO) personnel in performing their National Security and Emergency Preparedness (NS/EP) missions. Using the public switched network, it is intended for use when an emergency or crisis causes congestion and the probability of successful call completion is significantly decreased. "The GETS Concept," *available at* http://gets.ncs.gov/program_info.html. *See also* "ITU-T's Definition of NGN," *available at* http://www.itu.int/en/ITU-T/gsi/ngn/Pages/definition.aspx. The prioritization scheme should leverage and be interoperable with the National Communication System Industry Requirements for Next Generation Network-Government Emergency Telecommunications Service (NGN-GETS), to the extent feasible.

[42] 3GPP has formulated prioritization and QoS features for public safety LTE deployment. LTE Release 8, *supra* note 8. The commercial sector has not yet aggressively exploited these aspects of the LTE standard. However, public safety working groups, such as the National Public Safety Telecommunications Council (NPSTC) and the PSCR Demonstration Network Architecture Working Group are developing frameworks that would facilitate standards-based, interoperable solutions. *See generally*, NPSTC: "700 MHz Broadband Network Requirements Task Force," *available at* http://www.npstc.org/broadband.jsp. PSCR: "Public Safety 700-MHz Demonstration Network," *available at* http://www.pscr.gov/projects/broadband/700mhz_demo_net/700mhz_ps_demo_net.php. The

While the Commission should encourage innovation for all aspects of public safety LTE development, proprietary schema for features as critical to interoperability as prioritization and QoS may raise particular concerns. Proprietary features may inhibit competitors from offering similar features, preventing economic pricing, raising the costs for essential elements and for the network overall. The Commission should, therefore, play a key role in assessing the development and use of open versus proprietary mechanisms for these features, and any attendant effects on interoperability, and report on best practices in this area.

3. Performance and Coverage

The *Order/FNPRM* proposes to adopt operability and coverage requirements for public safety broadband networks.[43] As the Commission states, spectrum is a valuable resource requiring its efficient management.[44] In addition, the public safety broadband network must ultimately reach all of America, including urban, suburban, and rural areas and populations. State, local, Tribal, and Federal public safety users in rural areas, in particular, seek a public safety broadband network that will extend beyond typical market thresholds where "economic return" may become questionable.[45] Thus, coverage guidelines should be based on both population and geographic criteria. However, minimum data rates and coverage *requirements*,

---

PSCR LTE pilot program is studying Traffic Flow Templates for uplinks and downlinks that would include common settings for access class, access class barring, allocation/retention/priority, QoS class identifiers, and Access Point Names.

[43] *Order/FNPRM*, ¶¶ 59, 61, 71-73.

[44] *Order/FNPRM*, ¶ 59.

[45] *Order/FNPRM*, ¶ 73.

which deny the Corporation and affected State, local, and Tribal jurisdictions needed flexibility, may fall short on both counts.[46]

Instead, the Commission should set aspirational goals, not rigid mandates, for both data rates and coverage, at least initially. While it is possible that conflicts between such goals and the build-out will occur, such conflicts should be resolved by the Corporation in coordination with the Commission. For example, data rate obligations are likely to drive up costs and lead to decisions to shrink initial build-outs to smaller areas where such rates could be supported in violation of coverage rules. Moreover, implementing minimum data rate capabilities for initial build-outs, by providing a minimum data rate "safe harbor," will induce rapid obsolescence within the entire system and could necessitate replacement of through-put capacity before the Corporation can implement a robust unified nationwide system.

A successful nationwide and interoperable public safety broadband network needs flexibility to balance coverage and data rates to achieve efficient deployment within funding constraints. This requires consultation with affected States, localities,Tribes, and, where appropriate, Federal entities. These jurisdictions know the geography, density of population, and deployment schedule that would best serve both public safety and the general public. The network may also use deployable assets such as cells on wheels (COWs) and cells on light trucks (COLTs) to enhance coverage deficiencies or to replace stressed or damaged components. In this context, the Corporation should be responsible for devising any data rate performance specifications and validation methodologies, subject to Commission guidance.[47]

[46] *Order/FNPRM*, ¶¶ 59, 61, 71-73.

[47] *Order/FNPRM*, ¶ 62.

4. Coverage Reliability

The *Order/FNPRM* asks whether to impose coverage reliability requirements on the public safety network.[48] While the public safety broadband network should ultimately be at least as reliable as legacy land mobile radio and commercial broadband networks, the 95% coverage reliability benchmark that the *Order/FNPRM* proposes, while laudable, may be too rigorous to reasonably meet at the beginning of the nationwide network build-out.[49] The Corporation, however, should give serious consideration to meeting this goal over time given that this network will be used to protect life and property. A flexible, phased implementation would permit the Corporation, in consultation with State, local, and Tribal jurisdictions, to achieve such a goal over time.[50] Ultimately, the public safety broadband network will require uniform capability or designated surge capability to ensure coverage reliability and effective response in an emergency.

Additionally, indoor coverage requirements will vary according to specific needs.[51] Urban police and fire agencies, for instance, may have strict indoor coverage requirements. On the other hand, rural police, fire and emergency medical services, and agencies guarding border crossings, such as DHS Customs and Border Protection, may not. State, local, Tribal, and, where appropriate, Federal, jurisdictions are the best judges of indoor coverage needs in the portions of the RAN within their jurisdictions or mission. The Corporation, in cooperation with State, local,

---

[48] *Order/FNPRM*, ¶ 75.

[49] *Order/FNPRM*, ¶ 75.

[50] The Commission should clarify the meaning of "coverage reliability." "Coverage reliability" must take into account both the probability of successful message transmission and the extent that the system is available in a pre-defined geographic area. The Commission's definition appears to assume 100% system availability. *Order/FNPRM*, ¶ 75. Thus, for a selected geographic area that is fully built out, 95% coverage reliability would mean the ability to complete 95/100 call attempts.

[51] *See generally*, *Order/FNPRM*, ¶¶ 123-26.

Tribal, and, where appropriate, Federal jurisdictions, can address particular deficiencies as needed with follow-on network expansion/enhancement efforts, internal distributed antenna system approaches, potential future modifications to building infrastructure codes, and other mechanisms. The Commission, through the ERIC, should monitor and assess performance as the network matures.

5. Testing

The Commission seeks comment on whether and how to require conformance and interoperability testing.[52] The Administration believes the Commission should adopt rules requiring that equipment used in the network, both infrastructure and user devices, should be tested in accordance with both Corporation policy and developing testing regimes as described below.

Conformance testing of devices and network equipment ensures compliance with LTE standards at a base level.[53] With respect to LTE user devices, as the Commission notes, the PCS Type Certification Review Board (PTCRB) is establishing a Band Class 14 test suite for laboratory certification.[54] The *Order/FNPRM* proposes to require a certification that devices have gone through this process and a commitment to future testing as called for "within the certification process."[55] The PTCRB process provides for continual testing of new devices and software releases. The Commission should consider clarifying that the PTCRB process, including the requirement for continual testing of new devices and releases, is mandatory. This would provide a baseline for conformance testing for all public safety user equipment.

---

[52] *Order/FNPRM*, ¶ 106-115.

[53] *Order/FNPRM*, ¶ 106.

[54] *Order/FNPRM*, ¶ 107. Band Class 14 includes the public safety broadband spectrum.

[55] *Id.*

Moreover, the Corporation, with expert consultation as necessary, is best positioned to represent the interests of the public safety broadband network before the PTCRB.

With respect to LTE infrastructure equipment, the Multi Service Forum (MSF) is investigating the development of a framework for public safety infrastructure conformance and an LTE Interoperability Testing (IOT) and certification program for EPC primary IOT interfaces, including accreditation of testing facilities.[56] National, and many regional, commercial network operators maintain their own testing laboratories for infrastructure equipment. These laboratories enable commercial operators to ensure that software upgrades and new features do not disrupt interoperability or feature functionality. They could be venues for the actual conformance testing itself, so long as they are not affiliated with the providers of the equipment being tested, and can provide independent and unbiased certifications.[57] The Commission should conduct an assessment of the availability and accreditation of laboratories for IOT testing. Most importantly, the Commission should not permit any part of the public safety broadband network to go into operation until IOT is successfully completed via accredited laboratories on all equipment and devices using that infrastructure.

6. User Devices

The *Order/FNPRM* seeks comment on the use and required characteristics of devices on LTE networks.[58] The Administration believes that the Corporation should decide the characteristics of user devices after consultations with State, local, Tribal, and Federal entities, as well as device vendors and commercial roaming partners. The Corporation should take into

[56] *See generally*, "About MSF," *available at* http://www.msforum.org/about/index.shtml. The Corporation, with expert consultation as necessary, is best positioned to represent public safety broadband interests before this body.

[57] *Order/FNPRM*, ¶¶ 106-115.

[58] *Order/FNPRM*, ¶¶ 119-122.

account a number of factors, including the costs of additional functionality, time needed for training users, and support for: (1) legacy LMR networks; (2) 2G/3G/4G commercial wireless networks; (3) Wi-Fi; and (4) Bluetooth. With respect to channel bandwidth requirements, the Commission should require that public safety devices support 10+10 MHz, in addition to 5+5 MHz, given the current public safety spectrum allocation.[59]

The Commission should also conduct a more in-depth inquiry into the types of user devices that would best serve the public safety broadband network, including the value of encouraging or mandating public safety bands on commercial devices, as well as adding band classes in addition to Band Class 14, and Wi-Fi or Bluetooth, on public safety devices.[60] For public safety devices, multi-band capability would enable public safety users to roam onto commercial networks or to use WiFi or Bluetooth when the need arises.[61] The ability to roam onto commercial networks would permit public safety users to transition seamlessly to commercial networks before the public safety network is fully constructed or in cases of over-

[59] *Order/FNPRM*, ¶ 120. The President's Wireless Innovation and Infrastructure Initiative calls for reallocation of the D Block to public safety use, s*upra*note 5. The "D Block" refers to the 758-763 MHz and 788-793 MHz band adjacent to public safety 700 MHz radio frequencies.

[60] The Commission has a pending petition for rulemaking to require all 700 MHz mobile equipment to be capable of operating on all paired commercial 700 MHz frequency blocks. *See* Public Notice, "Wireless Telecommunications Bureau Seeks Comment on Petition for Rulemaking Regarding 700 MHz Band Mobile Equipment Design and Procurement Practices," RM No. 11592, DA 10-278 (rel. Feb. 18, 2010) (citing 700 MHz Block A Good Faith Purchaser Alliance Petition for Rulemaking Regarding the Need for 700 MHz Mobile Equipment to be Capable of Operating on All Paired Commercial 700 MHz Frequency Blocks (filed Sept. 29, 2009)), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-10-278A1.pdf. *See also* Public Notice, "Federal Communications Commission to Hold April 26, 2011 Workshop on the Interoperability of Customer Mobile Equipment Across Commercial Spectrum Blocks in the 700 MHz Band," RM No. 11592, DA 11-622 (rel. Apr. 7, 2011), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0407/DA-11-622A1.pdf. The Commission should open a rulemaking to include both 700 MHz commercial and public safety device interoperability.

[61] *Order/FNPRM*, ¶ 121.

loaded capacity.[62] Requiring the inclusion of public safety Band Class 14 on all commercial LTE devices could produce needed economies of scale for public safety users that would drive costs down. While there would be security risks in the mass production and sale of commercial devices carrying public safety frequencies, these are among the overall security concerns that will need to be addressed by the Commission and the Corporation.

The *Order/FNPRM* also asks about devices that offer multiple-mode support.[63] Manufacturers already are beginning to support multi-mode devices, including GSMGS/GPRS/E-GPRS, 1xRTT, 1xEV-DO, W-CDMA/HSPA, TD-SCDMA, and FDD-LTE.[64] Thus, additional regulation does not appear necessary to ensure multi-mode operations.[65] The Corporation should be supportive of device innovation occurring in the public and commercial sectors in meeting the operational requirements of the nation's first responders. Public safety should be able to benefit from new applications and other innovations being developed in the same way that the private sector is benefiting from an explosion in applications.

7. Deployable Assets

The Commission asks whether deployable assets operating in the public safety broadband spectrum should be required to comply with the technical and operational rules for that

[62] *Supra* note 39 (calling upon the Commission to consider how Wireless Priority Service, Government Emergency Telephone Service, and NGN Priority Service apply in a separate rulemaking to be conducted on public safety roaming onto commercial broadband networks.)

[63] *Order/FNPRM*, ¶ 122.

[64] *See, e.g.*, "Anritsu Introduces New Applications Test Solution Focused on Multi-Mode LTE Devices," *available at* http://www.14wfie.com/story/14299394/anritsu-introduces-new-applications-test-solution-focused-on-multi-mode-lte-devices.

[65] *Order/FNPRM*, ¶ 122. Satellite capability, while desirable, is likely cost prohibitive unless also implemented on commercial devices. In addition, other trade-offs, such as battery usage and slower data rates, might need to be considered.

spectrum.[66] The Administration agrees with the Commission that all deployable assets operating in the public safety broadband spectrum should comply with the technical and operational rules established for that spectrum.[67] The Corporation should capitalize on deployable assets to augment or replace existing infrastructure.[68] The ability to inject deployable assets such as COWS or COLTS or the abbreviated and typically less powerful "fly away kits" is often critical to successful relief operations.[69] The Commission should adopt rules that require the Corporation to test any such deployable capability in the lab and field for compliance with technical and operational rules and to ensure use of equipment that has been certified as previously discussed.[70]

8. Applications

The *Order/FNPRM* seeks comment on potentially requiring a common set of applications as a means to advance interoperability and, specifically, on mandating the five applications that the NPSTC Broadband Task Force recommended.[71] These applications appear, at least

[66] *Order/FNPRM*, ¶ 127 (citing National Broadband Plan at 318, Exhibit 16-B, *available at* http://www.broadband.gov/plan/16-public-safety/).

[67] *Order/FNPRM*, ¶ 128.

[68] The Corporation, in conjunction with State, local, and Tribal jurisdictions, should determine the type of backhaul such assets use, in accordance with user needs. *Order/FNPRM*, ¶¶ 127-128.

[69] *See generally*, Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), Pub. L. No. 110-53 §2201, 121 Stat. 266 (2007). Section 2201 of the 9/11 Commission Act amends the Public Safety Interoperable Communications Grants Program to require that grantees establish a strategic technology reserve to pre-position or secure communications for immediate deployment in a disaster.

[70] *See supra* Section II.C.5.

[71] *Order/FNPRM*, ¶ 55. These applications are: (1) Internet access; (2) Virtual Private Network (VPN) access to any authorized site and to home networks; (3) status or information homepage; (4) provision of network access for users under the Incident Command System; and (5) field-based server applications. National Public Safety Telecommunications Council, "700 MHz Public Safety Broadband Task Force

provisionally, to be necessary for the public safety broadband network. Federal first responders typically require capabilities such as Over the Air Service Programming (OTASP) and encryption rekeying of end user equipment.[72] Nevertheless, the Corporation, in consultation with State, local, Tribal, and Federal jurisdictions, can best assess the operational impacts of required applications or services. The Commission could best facilitate this effort by postponing any regulatory action in this regard and instead assessing at some later point whether the market is adequately addressing the need for various applications among affected jurisdictions.

D. Open Standards

Standards-based technologies provide a foundation and framework for achieving interoperability. Historically, proprietary technologies have impeded interoperability and competition for public safety applications.[73] Lack of standardization creates the potential for incompatible equipment and "Balkanized" service areas. It also decreases the pool of competitive vendors and tends to raise network and end-user costs. The Commission has taken a commendable first step by mandating an initial baseline of compatibility with LTE standards.[74] The Commission should also require that early adopters that have not implemented standards-based systems or that have adopted proprietary applications and architectures transition to open

---

Report and Recommendations" (NPSTC Broadband Task Force Report), § 6.3.2, at 20 (Sept. 2009), *available at* http://www.npstc.org/broadband.jsp.

[72] Open Mobile Alliance (OMA) working groups are developing standards for OTASP. These include Firmware Update Management Object (FUMO), a specification for updating the firmware of mobile devices over the air and Software Component Management Object (SCOMO), a specification that would permit software management of a remote device.

[73] Not every aspect of a public safety system requires standardization. The Commission must balance the public interest in stimulating innovative solutions when evaluating proprietary solutions.

[74] *Order/FNPRM*, ¶ 10.

standards, if such early implementation hinders nationwide interoperability.[75] Rather than mandating support for specific interfaces, which may evolve over time, the Commission should mandate compliance with LTE technical specifications, which are updated continually.[76]

E. IPv6

The Commission asks whether the entire public safety broadband network should be based on IPv6 from the outset.[77] The Corporation should adopt IPv6 as the network's baseline IP addressing scheme. Internet Protocol (IP) addresses available under IPv4, the system preceding IPv6, are depleting rapidly.[78] While there may be minor incremental costs to IPv6 deployment, the future savings from baseline implementation far outweigh these initial costs.[79]

F. Interconnection with Legacy Public Safety Networks

The Commission seeks comment on how to address interconnection of existing narrowband public safety networks ("legacy networks") with the public safety broadband

---

[75] Standards or implementation guidelines created by established bodies such as Third Generation Partnership Project (3GPP), Open Mobile Alliance (OMA), or Alliance for Telecommunications Industry Solutions (ATIS) are most appropriately applied to interfaces, or links between different components of a system, different components in a device, or different networks (narrowband and broadband).

[76] *Order/FNPRM*, ¶ 12. *See, e.g.*, 3G PP TS 23.401: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 10)" (Jan. 2011), *available at* http://www.3gpp.org/ftp/Specs/archive/23_series/23.401/.

[77] *Order/FNPRM*, ¶ 30.

[78] As of February 2011, the free pool of IPv4 addresses was depleted, with only regional free pools remaining available. "The IPv4 Depletion Site," *available at* http://www.ipv4depletion.com/?page_id=326. IPv6 provides for 128-bit IP addresses as opposed to the 32-bit addresses available under IPv4.

[79] Federal agencies that expect to use the public safety network are transitioning to an IPv6 format. Memorandum for Chief Information Officers of Executive Departments and Agencies from Vivek Kundra, Federal Chief Information Officer (Sept. 28 2010), *available at* http://www.cio.gov/Documents/IPv6MemoFINAL.pdf. *See also* "NTIA Convenes Stakeholders to Discuss IPv6 Deployment" (Sept. 28, 2010) *available at* http://www.ntia.doc.gov/press/2010/IPv6workshop_09282010.html.

network in the absence of the public safety partnership with the D Block operator.[80] NTIA supports the development of the capability to interconnect existing public safety Land Mobile Radio (LMR) to the broadband network for mission-critical voice.[81] Although progress has been made, LTE wireless broadband standards cannot yet meet the need for mission-critical voice communications.[82] Further, the country has invested billions of dollars in LMR network deployment.[83] Interconnecting the current communications systems to the future broadband network will maximize these investments while providing a migration path for future communications capabilities.[84] It will be important for public safety to develop capabilities to connect their LMR systems to the LTE network through solutions best suited for the situation.

However, at this initial stage of the development of LTE for public safety purposes, it is premature for the Commission to mandate particular gateways or forms of interconnection with

[80] *Order/FNPRM*, ¶ 58.

[81] NPSTC Broadband Task Force Report, *supra* note 71, § 6.2.10 at 14-14. NPSTC's Broadband Working Group is developing a functional definition of mission-critical voice. Mission-critical voice is generally thought to encompass "talk around" or the ability of radios to communicate outside of network infrastructure, "push to talk" or the ability to send messages via the push of a button instead of dialing, as well as other capabilities.

[82] For example, the DHS Office of Interoperability and Compatibility (OIC) proved this capability in the Radio Over Wireless Broadband demonstration. DHS, "Radio over Wireless Broadband Pilot Project Report" (July 2009) *available at* http://www.safecomprogram.gov/NR/rdonlyres/7FDFC2B3-1AF6-4F09-B672-8313F8CAE559/0/FINAL_ROWB_DC_PilotDHS_73109.pdf. *See also* "Demonstration shows that wireless broadband isn't just for data anymore" (Sept. 1, 2008) *available at* http://www.pscr.gov/about_pscr/press/broadband/leveraging_high-speed_networks_that_enable_ip-based_applications_092008-urgent_communications.pdf. *See generally*, DOC PSCR, "Radio over Wireless Broadband: Project Description" *available at* http://www.pscr.gov/projects/broadband/row-b/row-b.php. The DHS OIC Voice Over Internet Protocol Working Group continues to study these issues.

[83] For example, DOJ's Integrated Wireless Network program is a state-of-the-art land mobile radio system that is used by Federal and other public safety agencies, such as DOJ, DHS, the U.S. Park Service, and even Canadian law enforcement, in certain parts of the country, including border areas.

[84] Conceivably, once LTE mission-critical voice capabilities are operational, public safety users would be able to use LMR and LTE voice interchangeably during a transition period, ensuring a graceful and secure migration.

legacy voice systems. Since the LTE standard does not cover this linkage, the Commission should be particularly cautious in permitting solutions that are not based on open standards. Before approving proprietary solutions, the Commission should assess the availability of both open standard and proprietary gateway solutions, as well as the impact of non-standard gateways on overall interoperability.

G. Base Station Out-of-Band Emission Limits

The *Order/FNPRM* tentatively concludes that a limit on out-of-band emissions of 43+10 Log (P) dB for operations in the 763-768 MHz band and the 793-798 MHz band would protect against public safety broadband network adjacent band interference.[85] The proposal would result in a limit on out-of-band emissions of -13 dBm as measured in a 100 kHz resolution bandwidth.[86] The out-of-band emission limit referenced to a bandwidth of 6.25 kHz is -25 dBm.[87] In contrast, the LTE standard specifies a limit of only -46 dBm for spurious emissions from base stations using a 6.25 kHz resolution bandwidth.[88] Even though the *Order/FNPRM* indentifies other measures to reduce the impact of interference to mobile wireless systems, the proposed out-of-band emission limits would unreasonably increase the potential for interference. The Commission therefore should reduce the limits to be consistent with the level specified in

[85] The out-of-band emission levels are measured using a resolution bandwidth of at least 100 kHz. However, a resolution bandwidth of 30 kHz may be employed in the regions 100 kHz outside and adjacent to the band.

[86] The 43 + 10 Log (P) results in a limit of -43 dBW for out-of-band emissions, which is equal to -13 dBm as measured in a 100 kHz bandwidth.

[87] -13 dBm/100 kHz + 10 Log (6.25/100) = -25 dBm.

[88] 3GPP TS 36.104, "3rd Generation Partnership Project: Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception" (Release 8) (Dec. 2010) § 6.6.4.3.1, *available at* http://www.3gpp.org/ftp/Specs/archive/36_series/36.104/36104-8b0.zip.

the LTE technical specifications.[89] In addition, there is a potential for second harmonic interference to Global Positioning System (GPS) receivers operating in the 1559-1610 MHz band. The Commission should work with NTIA to ensure that that the Commission adequately addresses harmonic interference to GPS.[90]

H. Interference Coordination

The *Order/FNRPM* asks for input on the need for interference mitigation requirements.[91] In single frequency re-use systems such as that proposed for public safety, the potential for adjacent cell interference requires coordination between neighboring cells. While LTE provides a minimum coordination methodology, as the Commission recognizes, solutions in addition to Static Inter-cell Interference Coordination are available.[92] Fractional frequency re-use, particularly in controlling cell edge performance, is one such option.[93] To the extent that potential interference exists among cells in the nationwide system, the Corporation would be responsible for designing the network to mitigate this effect. With respect to potential interference from and into the adjacent systems of commercial operators, the optimum interference mitigation methodology may vary with particular circumstances, and should be left to the Corporation. The Commission should, however, require coordination between the public

[89] *Order/FNPRM*, ¶ ¶ 51-55.

[90] Transmitters in the 788-798 MHz band would generate second harmonic emissions in the 1576-1596 MHz band.

[91] *Order/FNPRM*, ¶ 78.

[92] Ericsson Contribution R1-061374, TSG-RAN WG1 #45 (Shanghai, China) (May 8-12, 2006), *available at* http://www.3gpp.org/ftp/tsg_ran/WG1_RL1/TSGR1_45/Docs/R1-061374.zip; Ericsson Contribution R1-061375, TSG-RAN WG1 #45 (Shanghai, China) (May 8-12, 2006) *available at* http://www.3gpp.org/ftp/tsg_ran/WG1_RL1/TSGR1_45/Docs/R1-061375.zip.

[93] Fractional frequency reuse allows more sub-channels to operate at the cell center, an area relatively less susceptible to interference, than at the cell edge.

safety broadband system and adjacent commercial systems as is the case now between commercial systems.[94]

I. Security and Encryption

As the Commission states, secure communications are vital to public safety.[95] The Commission should adopt as requirements its proposed service features with respect to communications security and encryption, as they likely will be sufficient to address Federal first responder requirements and concerns.[96] As a general matter, Federal law enforcement users require and expect encryption of messages (voice and data), mutual authentication, VPN tunnels, and other features that enhance and ensure the security of the transmitted communications. Federal users accessing the public safety broadband network will require system-level security capabilities (which may be transparent to the end user). The LTE standard supports such requirements through an air interface and through VPN technologies, thus providing flexibility in meeting security needs.[97] In addition, the LTE standard provides proper mechanisms for authentication of not only the devices on the network, but also the users of the devices.[98]

---

[94] *Order/FNPRM*, ¶¶ 78-79.

[95] *Order/FNPRM*, ¶ 65.

[96] *Order/FNPRM*, ¶¶ 65-69.

[97] *See, e.g.*, 3GPP TS 33.401, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture" (Release 8), *available at* http://www.3gpp.org/ftp/Specs/archive/33_series/33.401/33401-870.zip. "Tunneling" provides a secure path through a non-secure network. Specific decisions on tunneling protocols should be left to the Corporation. *Order/FNPRM*, ¶ 31.

[98] 3GPP TS 33.102 v 8.6.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture" (Release 8), § 5.1.2 , *available at* http://www.3gpp.org/ftp/Specs/archive/33_series/33.102/33102-860.zip. As public safety's needs evolve, the Corporation can turn to requirements-development groups such as the NPSTC Broadband Task Force and standards bodies such as 3GPP in collaboration with ATIS to help find solutions to meet these needs.

J. Fixed Services

The Commission proposes to allow fixed use in the 763-768 MHz and 793-798 MHz bands only on an ancillary basis.[99] The Administration supports the Commission's proposal. The Commission allocated this band to mobile services and the State, local, Tribal, and Federal public safety, emergency, and public safety support services that should use it will, at times, have large capacity requirements for mobile use. These mobile needs should take precedence over fixed uses in cases of over-loaded capacity. As the Commission recognizes, bands other than the 700 MHz public safety broadband spectrum are available for public safety fixed use, including the 4940-4990 MHz band (4.9 GHz). Therefore, the Commission should allow fixed uses in public safety 700 MHz broadband spectrum only on an ancillary basis.

K. Federal Use

Federal public safety entities interoperate with their State, local, and Tribal counterparts, especially during emergencies, natural and man-made disasters, and other extreme circumstances.[100] The Commission has wisely determined to preserve the existing principle of

---

[99] *Order/FNPRM*, ¶¶ 129-31.

[100] *See generally*, Comments of the National Telecommunications and Information Administration, PS Docket No. 06-229 (Nov. 9, 2009)) *available at* http://www.ntia.doc.gov/filings/2009/FCC_PS06229_700MHz_091109.pdf. Federal agencies share information, infrastructure, and systems with State and local public safety agencies. *See, e.g.*, "Interoperability Montana Project," http://interop.mt.gov/. When the I-35W Bridge collapsed in Minneapolis, 2007, the Coast Guard, FBI underwater search and evidence response (USERT) and US Naval Sea Systems Command (NAVSEA) mobile diving and salvage teams mobilized to support recovery operations. *See* National Transportation Safety Board, "Collapse of Highway I-35W Highway Bridge, Minneapolis, Minnesota" (Aug. 1, 2007) at 4, *available at* http://www.dot.state.mn.us/i35wbridge/ntsb/finalreport.pdf ("I-35W Report"). The United States Marine Corps deployed the Department of Defense's (DOD's) East Coast Rapid Response System (RRS), a transportable system that operates in public safety land mobile radio bands, to support Hurricane Katrina and Tropical Storm Cindy relief efforts. At the request of State officials, DOD has deployed on air, sea and land to help fight California fires. "Defense Department Continues Aid on California's Fire Front," *available at* http://www.defense.gov/news/newsarticle.aspx?id=47903. *See also* DOD Directive No. 3025.15 (Feb.18, 1997*)* (military assistance to civil authorities for civil disturbances, acts of terrorism, disasters); Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. §§ 5121-5207

Federal eligibility to use the public safety broadband network.[101] The Commission asks what the appropriate service arrangements for Federal agencies should be and whether the existing framework, under which the Public Safety Broadband Licensee has a central role in authorizing Federal access, should be retained in light of "the revised network of networks approach."[102]

Federal agency administration and procurement of assets are generally centralized. Federal agencies will require a single point of contact for making service arrangements on the public safety broadband network. This central contact should reside with the Corporation. Standardized agreements with appropriate local schedules could help streamline Federal procurement and realize savings through economies of scale.[103] Federal users serving similar public safety functions and taking similar service should not have to pay more than their State, local, or regional partners. Capacity and coverage bear on the types of service arrangements that the Corporation will offer.[104] In addition, Federal missions and geographic diversity require flexibility in the types and terms of services offered.[105] The Corporation should offer Federal

---

("Stafford Act") (Presidential authority to issue major disaster declarations authorizing Federal aid to States). *See* http://www.fema.gov/about/index.shtm (The Federal Emergency Management Agency (FEMA) of the Department of Homeland Security principally administers the Stafford Act and maintains the National Response Framework (comprehensive, coordinated approach to a domestic incident involving responders of all jurisdictional levels)).

[101] *Order/FNPRM*, ¶ 100 (Commission has determined that "Section 337 of the Act does not bar Federal government public safety entities from using the 700 MHz band under certain conditions.")

[102] *Order/FNPRM*, ¶¶ 100-03. 47 C.F.R. § 2.103(c).

[103] The ECPC, in its role as Federal clearinghouse and coordinator for operable and interoperable communications, and with the input of the IRAC, can facilitate such agreements at the request of the Corporation and Federal agencies.

[104] The Administration expects that capacity issues will be addressed in the nationwide prioritization framework and the use of it as determined by particular jurisdictions.

[105] Some Federal agencies' communications and operational needs require a portfolio of differing spectrum bands with different propagation characteristics from the 763-768 MHz and 793-798 MHz

partners a variety of service options, including subscribership, leasing, or sharing infrastructure, to meet some of their communication needs. For Federal agencies choosing to subscribe to the network, contracts should permit local, regional, or nationwide purchase options.

Regardless of the type of arrangement, Federal missions often require superior quality of service standards, so that Federal entities taking service will likely need at least the same QoS standards and prioritization scheme as their State, local, and Tribal counterparts subject, in emergencies, to the decisions of the incident commander.[106] The Commission should permit Federal entities that meet the purpose of Section 337(f) access to the public safety network, subject to the approval of the Corporation in consultation with State, local, and tribal jurisdictions.[107] However, because a single nationwide public safety broadband network does not require intra-system roaming, once a Federal agency becomes a subscriber on the nationwide network, it should not have to pay roaming charges.[108]

---

bands alone. This mission diversity means that Federal agencies will not necessarily forego Federally-allocated spectrum should they decide to use the public safety broadband network.

[106] *See* Federal Emergency Management Agency, "Incident Command System (ICS)," *available at* http://www.fema.gov/emergency/nims/IncidentCommandSystem.shtm. *See also* Department of Commerce, *Federal Strategic Spectrum Plan* (Mar. 2008), at 4, B137-139, B-143, *available at* http://www.ntia.doc.gov/reports/2008/FederalStrategicSpectrumPlan2008.pdf (increasing Federal broadband requirements); Department of Commerce, *Spectrum Policy for the 21st Century: A Public Safety Sharing Demonstration* (May 2007), at xiv, *available at* http://www.ntia.doc.gov/reports/NTIAWARNReport.pdf (the Washington, DC Wireless Accelerated Responder Network, a 700 MHz broadband pilot demonstrated a critical value in supporting both Federal and non-Federal agencies' broadband communications needs).

[107] *See* Letter to the Hon. Julius Genachowski, Chairman, Federal Communications Commission from Lawrence E. Strickling, Assistant Secretary for Communications and Information, NTIA (Apr. 8, 2011) *available at* http://www.ntia.doc.gov/filings/2011/NTIALetter_PS06-229_04082011.pdf (supporting City of Charlotte, North Carolina Request for Declaratory Ruling, PS Docket No. 06-229 (Mar. 7, 2011)). While the Commission also correctly points to potential capacity issues from Federal entities' and/or public safety support service providers' use, the Corporation and, where appropriate, the incident commander, would be best positioned to strike the most appropriate balance with respect to access and usage, depending upon the specific circumstances. *See Order/FNPRM*, ¶ 102.

The Commission also asks whether there should be constraints on how revenues from Federal agencies are spent, and how this should be monitored and enforced.[109] For consistency with the statute allocating 700 MHz public safety spectrum, the Commission should not permit the Corporation or any State, local, or Tribal jurisdiction to divert funds collected from Federal agencies for use of public safety broadband spectrum to non-public safety broadband network purposes.[110] Agencies should remit fees to a single central entity, either the Corporation or a clearinghouse selected by the Corporation. The Commission should impose reporting and audit requirements on the Corporation with respect to the collection and disbursement of fees and other revenues.

L. Public Safety Broadband and Next-Generation 911 Networks

The Public Safety Answering Point (PSAP) provides a vital link between a person in need of assistance and the first responder community. Generally, the PSAP dispatcher relies on speech from a person in distress to interpret situational awareness. The dispatcher relays that information to the first responders. The Administration is currently addressing migration to next-generation technologies that permit the public to communicate with the PSAP by other modes of communication such as text, images, and video, to enable "a faster, more focused response."[111]

---

[108] However, if a Federal user/agency chooses to take service on a local or regional basis, or buys another service option which does not extend throughout the nation, additional charges could apply for service outside the contractually covered territory.

[109] *Order/FNPRM*, ¶ 103.

[110] Congress has made separate allocations of 700 MHz spectrum for public safety and commercial use. 47 U.S.C. § 337 (a). The Commission has long-permitted non-commercial licensees to recover their costs from users. *See, e.g.*, 47 U.S.C. § 90.179 (g) (permitting sharing with Federal Government entities on a non-profit, cost-shared basis).

[111] *Order/FNPRM*, ¶ 133. NTIA and the National Highway Traffic Safety Administration, working through the E-911 Implementation Coordination Office, submitted to Congress a plan for migrating to a

The *Order/FNPRM* asks how best to ensure that the public safety broadband network can connect with Next-Generation 911 (NG911) networks, improving public safety agencies' situational awareness and enabling a faster, more focused response.[112] Currently, 911 PSAPs transmit voice communications according to common technical standards. The 3GPP community and other standards groups are beginning to develop technical standards that would allow access to non-voice emergency services (citizen to PSAP) as well.[113] With respect to representation before such standards bodies, the Corporation, with appropriate technical consultation, should participate in such activities. This would ensure that common standards are developed to serve the needs of citizens and of the public safety community as a whole.

M. Section 337 Eligible Users

The Commission's tentative conclusion remains that use of the 700 MHz band should be limited to entities whose "'sole or principal purpose' is to 'protect the safety of life, health, or property' and who meet the remaining requirements of Section 337(f)."[114] This is based on the Commission's efforts to ensure that services in the 700 MHz band conform to all of the elements

---

national IP-enabled emergency network capable of receiving and responding to all citizen-activated emergency communications and improving information sharing among all emergency response entities. *See* "A National Plan for Migrating to IP-Enabled 911 Systems" (Sept. 2009), *available at* http://www.911.gov/pdf/National_NG911_Migration_Plan_FINAL.pdf. Further, next generation technologies will provide other forms of communications that may be better suited for persons with disabilities. Framework for Next Generation 911 Deployment, *Notice of Inquiry*, PS Docket No. 10-255, 25 FCC Rcd 17869, 17874 (2010).

[112] *Order/FNPRM*, ¶ 133. The Commission has recently launched a comprehensive inquiry on how to facilitate a transition to NG-911. Framework for Next Generation 911 Deployment, 25 FCC Rcd 17869 (2010).

[113] There may also be cost benefits for the public safety broadband network in leveraging high-speed bandwidth connections between existing PSAPs.

[114] *Order/FNPRM*, ¶¶ 134-35.

of the statutory definition of "public safety service."[115] Nevertheless, the Commission recognizes

> the strong desire of many in the public safety community to include secondary users such as utilities, public works and others on their network as a mechanism to coordinate common activities and respond jointly to emergencies, as well as a method to spread costs and capitalize on infrastructure sharing opportunities.[116]

As an initial matter, NTIA believes that uses of the 700 MHz public safety spectrum should not be limited to those involving police, fire, and medical personnel who have as their sole or principal purpose the protection of public safety, health, or property. In this context, the term "secondary use" does not adequately describe the role of non-traditional public safety users during certain emergencies, and NTIA appreciates the Commission's willingness to revisit Section 337 eligibility.[117]

As long as the use of the 700 MHz band is consistent with the statutory purpose of Section 337, to protect the safety of life, health, or property, the Commission should permit use of the band by non-traditional public safety agencies. For example, it could be essential for a commercial utility to use the 700 MHz band if power lines are down and life and property are at risk. Yet the use of the 700 MHz band by the same commercial utility company to read meters would not be permitted because that use does not conform to the statutory purpose. The

---

[115] Service Rules for the 698-746, 747-762 and 777-792 Bands; Implementing a Nationwide, Broadband Interoperable Public Safety Network in the 700 MHz Band, *Third Further Notice of Proposed Rulemaking*, 23 FCC Rcd 14301, 14401-14407, at ¶¶ 312-327.

[116] *Order/FNPRM*, ¶ 135.

[117] NTIA recommends avoiding the term "secondary" when referring to use by critical infrastructure, transportation agencies, and similar organizations under the direction of an incident commander. For the success of the overall response, and the safety of responders' lives, these organizations' access in an incident should be equal to that of their State and local partners. "Public safety support providers" include those whose primary mission might not fall within the classic public safety definition, but who may provide vital support to the general public and/or the public safety official. SAFECOM, "Frequently Asked Questions,"*available at* http://www.safecomprogram.gov/SAFECOM/about/faq/#1126. NTIA recommends use of this term instead.

Commission should interpret Section 337 broadly to allow access to the 700 MHz band for *communications* whose sole or principal purpose is to protect the safety of life, health, or property, at the discretion of the incident commander.

To illustrate this point, public safety support providers, *i.e.*, providers of critical infrastructure, public works, and road crews and transportation authorities, can ensure the effectiveness of an emergency response.[118] For example, FEMA's comprehensive National Response Framework (NRF) for emergency operations includes a range of Emergency Support Functions (ESFs) that an incident response may entail.[119] In the 2007 Minneapolis bridge collapse, the State Department of Transportation (DOT) developed and implemented detours to accommodate displaced traffic and later assisted in the recovery of damaged infrastructure.[120] On FEMA's Urban Search and Rescue Teams, fire, law enforcement, Federal and local government, and private company personnel partner to help locate victims and manage recovery operations.[121] Such responders' support is critical to containment of, and recovery from, emergencies and entitles them to access and use of the public safety broadband network, subject

[118] *See generally*, FCC Wireless Telecommunications Bureau: "Staff Paper, Private Land Mobile Radio Service: Background" (Dec. 18, 1996) at 9, *available at* http://wireless.fcc.gov/reports/documents/whtepapr.pdf.

[119] The NRF establishes a comprehensive, national, all-hazards approach to domestic incident response, which describes how communities, tribes, States, the Federal government, private sectors, and non-governmental entities work together to coordinate a response. Emergency Support Functions (ESFs include, in addition to communications, infrastructure protection and emergency repair, infrastructure restoration, oil and hazardous materials response, environmental short- and long-term cleanup, energy infrastructure assessment, repair and restoration, energy industry utilities coordination, and support to access, traffic, and crowd control. *See generally*, FEMA,"Emergency Support Function: Annexes," *available at* http://www.fema.gov/pdf/emergency/nrf/nrf-esf-intro.pdf. Many States and local governments have similar structures. *See, e.g.*, Florida Division of Emergency Management, "Florida Disaster," http://www.floridadisaster.org/EMTOOLS/esf.htm.

[120] *See* I-35W Report, *supra* note 106.

[121] FEMA: "US&R Participants," *available at* http://www.fema.gov/emergency/usr/participants.shtm.

to appropriate prioritization.[122] For the success of the overall operation and safety of all responders, where the incident commander requires their help and connectivity, their communications status must be equal to that of other comparable first responders, as determined by the incident commander or determined by the policies of the Corporation. And to be prepared adequately, such status must include the ability to train on, and use the public safety broadband network in, non-emergency conditions.

Moreover, economic sustainability is as crucial a factor to the operability of a new public safety broadband network as are common technical standards and coherent network architecture.[123] Allowing use by responders of utilities and public works can help "spread costs and capitalize on infrastructure sharing opportunities."[124] For this additional reason, the Commission should permit the Corporation, in consultation with State, local, and Tribal jurisdictions, to offer service to public safety support providers.

CONCLUSION

NTIA applauds the Commission's efforts to address the critical need for public safety broadband services. The Nation is at the threshold of a new generation in public safety communications. These vital communications require a nationwide architecture. A nationwide public safety broadband architecture allows for the cost-effective sharing of core resources. It

[122] The Commission's D Block rules, now stayed, permitted the commercial D Block operator to use public safety broadband spectrum. 47 CFR § 90.1407 (c); *Order/FNPRM*, n. 34. The national operator should set the prioritization framework, in consultation with local, State, and Tribal jurisdictions. *See supra* Section II.B.3. The incident commander would potentially assign users and applications in real time according to the nationwide scheme.

[123] *See* FCC, "A Broadband Network Cost Model: A Basis for Public Funding Essential to Bringing Nationwide Interoperable Communications to America's First Responders" (May 2010), *available at* http://www.fcc.gov/pshs/docs/ps-bb-cost-model.pdf.

[124] *Order/FNPRM*, ¶ 135. *See* FCC, "National Broadband Plan," Recommendation 12.4, *available at* http://www.broadband.gov/plan/12-energy-and-the-environment/#r12-4 ("[A]lthough the network will take years to build, carrying critical traffic from multiple users can help lower costs for all").

enables early deploying jurisdictions to focus limited resources on the build-out of a more robust Radio Access Network. And it simplifies harmonization and adaptation to technology updates. The Administration believes that an expert and empowered Corporation should be tasked with and capable of making key technical, planning and operational decisions in consultation with relevant local, State, and Tribal jurisdictions, and where appropriate, Federal entities.

Under a patchwork quilt of networks approach, each individual network would not only have to purchase each and every network element and harmonize it with every other network configuration, each network would have to regression test every technology update against all other network configurations. These are virtually impossible tasks to manage, and unnecessary barriers to interoperability.

Federal entities are important partners in State, local, Tribal, and regional emergency and public safety response. As the Commission has repeatedly said, they are eligible to use the public safety broadband network. The Commission also should acknowledge the critical role public safety support services, such as nuclear and power plant relief and recovery personnel, transportation agencies, and road crews, often play in emergency response. Subject to prioritization, they should be allowed to access the public safety broadband network. The Commission should permit the Corporation to approve Federal agency and public safety support service use, in consultation with affected State, local, and Tribal jurisdictions.

Respectfully submitted,

Kathy D. Smith
Chief Counsel

Lawrence E. Strickling
Assistant Secretary for Communications
and Information

Anna M. Gomez
Deputy Assistant Secretary for
Communications and Information

National Telecommunications
and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4713
Washington, DC 20230
(202) 482-1850

June 10, 2011