

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:)
)
)
Public Safety and Homeland Security Bureau) PS Docket No. 06-229
Seeks Comment on Interoperability, Out of)
Band Emissions, and Equipment)
Certification For 700 MHz Public Safety)
Broadband Networks)
)
)

COMMENTS OF AT&T, INC.

Robert Vitanza
Gary L. Phillips
Paul K. Mancini
AT&T Inc.
1120 20th Street, N.W.
Washington, DC 20036
(202) 457-3076
Counsel for AT&T Inc.

July 19, 2010

EXECUTIVE SUMMARY

The Commission's decision to allow certain public safety entities to begin construction of local and regional 700 MHz mobile broadband networks was an important step towards realizing the Commission's goal of facilitating the creation of a nationwide interoperable public safety broadband network—a vision shared by AT&T. In these comments, AT&T offers its opinions on the questions posed by the Commission about how to enable the development of public safety networks that are robust, sophisticated and, most importantly, interoperable.

AT&T believes that the Commission can best facilitate the development of interoperable public safety broadband networks by promoting a standards-based approach to public safety network development that is centered around implementation of the 3GPP LTE specifications and the leveraging of commercial technologies and infrastructures wherever appropriate. In addressing any technical questions, the Commission should always strive to impose only the minimum regulatory obligations required to ensure interoperability. Accordingly, AT&T offers the following recommendations:

- Provided that baseline operational requirements—such as the use of the LTE protocol, the provision of Internet access, and VPN support—are maintained, adoption of a detailed list of application requirements is unnecessary for the purposes of interoperability and should be avoided.
- To support roaming, all public safety devices should support 3GPP Band 14 and be free to fall back to the 3G networks of commercial providers to complement their LTE operations.
- Priority access mechanisms should be based on existing systems or those currently under development and the Commission should promote priority access models that are voluntary and receive Federal funding.
- Questions of system characteristics, interfaces, testing and security should, to the extent possible, be resolved by reference to and reliance upon standards and recommendations, such as those developed by NIST, ATIS, 3GPP and other such organizations.
- The need for network performance, reliability, capacity and coverage will vary among public safety entities and thus should be left to their discretion.

- Rather than requiring the development of a nationwide core for public safety broadband networks, the Commission should recognize that interconnection and roaming can most easily and efficiently be accomplished by leveraging commercially available networks and databases on a regional basis.
- The Commission should defer to public safety network operators' judgment on matters of network OA&M and governance procedures. Although the Commission and the ERIC can usefully act as forums for standardization and can provide recommendations, no Federal mandates in these areas should be issued.
- The Commission should apply the general $43 + 10 \log P$ OOB limit to public safety broadband networks and should review the entire 700 MHz OOB framework to resolve apparent inconsistencies therein.
- Public safety broadband devices should embrace the technical parameters of the 3GPP Release 8 LTE specifications and should be subject to Commission and industry recognized certification processes.

Each of these recommendations is based upon the belief that allowing public safety licensees maximum flexibility to design and operate their own systems, confined by a limited set of basic interoperability requirements, will most effectively promote the rapid and organic development of wireless broadband networks that are best suited for public safety needs.

Nevertheless, the most important action the Commission can take to assist in the development of highly advanced and interoperable public safety wireless broadband networks is to support public safety's efforts to seek a reallocation of the Upper 700 MHz D Block spectrum for public safety use. The D Block spectrum will be essential to the future development of public safety broadband networks and will be particularly crucial during times of high traffic, when many public safety users from outside the incident area may be roaming on a single local or regional network. Reallocation of the D Block spectrum will assist in a number of the technical and interoperability challenges discussed below, and will also provide the best "bang for the buck" for public safety by ensuring cost effective, robust and reliable networks develop that will continue to satisfy public safety demands into the foreseeable future.

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	i
I. INTRODUCTION	2
II. INTEROPERABILITY.....	5
A. Applications	5
B. Roaming	6
C. Priority Access	9
D. System Characteristics, Interfaces and Testing	11
E. Security	12
F. Performance, Reliability, Capacity and Coverage	13
G. Nationwide Core	14
H. Network Operations, Administration and Maintenance (OA&M)	17
I. Governance	17
III. OUT-OF-BAND EMISSIONS	18
IV. EQUIPMENT CERTIFICATION	19
V. CONCLUSION.....	21

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:)	
)	
)	
Public Safety and Homeland Security Bureau)	PS Docket No. 06-229
Seeks Comment on Interoperability, Out of)	
Band Emissions, and Equipment)	
Certification For 700 MHz Public Safety)	
Broadband Networks)	
)	
)	

COMMENTS OF AT&T, INC.

AT&T, Inc. (“AT&T”) hereby submits its comments in response to the Public Notice released by the Federal Communications Commission (“Commission”) seeking comment on interoperability, out-of-band emissions, and equipment certification for 700 MHz public safety broadband networks.¹ AT&T applauds the Commission on its order granting the requests for waiver of various public safety agencies to allow for the early deployment of local and regional 700 MHz public safety wireless broadband networks.² In these comments, AT&T urges the Commission to maximize waiver recipient flexibility, but nevertheless ensure that public safety networks are interoperable and benefit from commercial economies of scale and scope. To do so, the Commission should adopt the least intrusive technical requirements that are based on the

¹ Public Safety And Homeland Security Bureau Seeks Comment on Interoperability, Out of Band Emissions, and Equipment Certification for 700 MHz Public Safety Broadband Networks, *Public Notice*, DA 10-884, PS Docket 06-229 (rel. May 18, 2010) (“*Public Notice*”).

² See Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks, PS Docket 06-229, *Order*, 25 FCC Rcd 5145 (2010) (“*Waiver Order*”).

standards for the Long Term Evolution (“LTE”) air interface protocol³ and are narrowly-focused on interoperability. Additionally, AT&T renews its support of public safety’s efforts to promote a reallocation of the Upper 700 MHz D Block spectrum.

I. INTRODUCTION

On May 13, 2010, the Commission released an order granting waivers to twenty-one public safety entities to allow them to begin construction of local and regional mobile broadband networks on the 700 MHz public safety broadband spectrum (763-768 MHz and 793-798 MHz).⁴ By enabling early build-out, the Commission hopes to allow public safety agencies to participate in the ongoing development process for 4G mobile broadband technologies, take advantage of funding opportunities, and leverage existing deployment plans.⁵ The Commission subjected the waivers to various conditions meant to ensure that local and regional public safety networks are interoperable with the nationwide 700 MHz public safety broadband network still to be constructed. Among the conditions placed on the waiver recipients are requirements that the networks operate with the LTE air interface protocol, specifically the Third Generation Partnership Project (“3GPP”) Standard, Evolved Universal Terrestrial Radio Access, Release 8, that all waiver recipients enter into a spectrum lease with the 700 MHz Public Safety Broadband Licensee, the Public Safety Spectrum Trust (“PSST”), that all networks support a limited number

³ An air interface is the standard operating system of a mobile network that ensures compatibility between devices and base stations and facilitates wireless communications.

⁴ *See Waiver Order.*

⁵ *Id.* at 4-5, ¶ 10.

of basic uniform applications (e.g., Internet access, VPN⁶), and various other technical and operational limitations.⁷

Although several key requirements for interoperability were set forth in the *Waiver Order*, in the instant *Public Notice* the Commission seeks further comment on specific issues related to interoperability, out-of-band emissions, and equipment certification for use in crafting its final rules for the public safety broadband network. AT&T applauds the light-touch requirements for interoperability that the Commission articulated in the *Waiver Order* as the correct approach for the public safety broadband systems. For resolving the remaining technical issues, AT&T urges the Commission to continue to apply a light-touch and, except for basic minimum standards to promote interoperability, allow local and regional public safety agencies to deploy those features and capabilities that they determine are best suited and cost-justified for their local or regional public safety broadband network. The basic minimum standards for all public safety broadband networks should be based upon the LTE standards, which will best serve the goal of interoperability, allow for public safety to take advantage of the economies of scale and scope driven by commercial standards-based equipment, and enable a quick, robust deployment of public safety broadband networks.

As the Commission appropriately recognized in the *Waiver Order*,⁸ there are significant advantages to the adoption of LTE as the uniform standard for all 700 MHz public safety broadband networks. LTE, which has been endorsed by major representatives of public safety

⁶ A VPN, or Virtual Private Network, provides remote access to the private applications, content or network services of an organization over the public Internet in a highly secure way through the use of encryption and authentication techniques.

⁷ *Waiver Order* at 8-22, ¶¶ 20-64.

⁸ *Id.* at 13-14 ¶ 38.

users such as the National Public Safety Telecommunications Council (“NPSTC”),⁹ the Association of Public-Safety Communications Officers (“APCO”),¹⁰ and the PSST,¹¹ will provide true broadband capabilities to the public safety community. By mandating a uniform protocol, the Commission has not only taken a major step towards ensuring interoperability, it has given public safety the ability to take advantage of commercial economies of scale in procuring network infrastructure and devices. Moreover, as LTE has generally emerged as the consensus protocol for commercial 700 MHz networks, its adoption for the public safety broadband network will allow public safety to take advantage of ongoing commercial deployment through roaming or other innovative public-private partnerships.

In this proceeding, the Commission should establish minimum requirements for interoperability, not specific features and functionalities of the public safety broadband networks. As the Commission indicated in the *Waiver Order*, by adopting LTE as the public safety broadband protocol, the Commission has given public safety an opportunity to participate in and shape the ongoing 4G development process to ensure that the emerging standards are suitable for public safety needs. Accordingly, the Commission must provide sufficient flexibility to allow experimentation and participation by these entities, so long as they conform to the minimum requirements needed for interoperability. Adopting Commission mandates that exceed these minimum requirements and vary from the LTE standards might have the undesired effect of

⁹ Comments of National Public Safety Telecommunications Council, PS Docket No. 06-229 at 6 (filed Oct. 16, 2009).

¹⁰ Reply Comments of APCO, PS Docket No. 06-229 at 2 (filed April 16, 2010) (“LTE is the unanimous choice of public safety users and all current 700 MHz commercial licensees for a standard broadband technology.”).

¹¹ See Public Safety Spectrum Trust Ex Parte Filing, PS Docket 06-229 (Dec. 15, 2009) (entering into the docket National Public Safety Telecommunications Council, 700 MHz Public Safety Broadband Task Force Report and Recommendations (2009) (“*NPSTC BBTf Report*”)).

discouraging some state and local public safety entities from deploying wireless broadband because of prohibitive increases in cost and complexity.

II. INTEROPERABILITY

As indicated above, AT&T urges the Commission to remain focused on LTE in setting the minimum requirements for interoperability for the public safety broadband network. Public safety network operators require sufficient flexibility to build a network that is responsive to their local needs, but guided by the basic LTE framework to create cost-saving economies of scale and ensure interoperability.

A. Applications

As the Commission correctly recognized in the *Waiver Order*, there is a small number of operations that all public safety broadband devices should support as a function of interoperability and baseline utility. For example, all devices should support Internet access and VPN access. Provided that baseline operational requirements—such as use of the LTE protocol, adherence to other 3GPP standards and the provision of Internet access—are maintained, adoption of the detailed list of application requirements recommended in the NPSTC Broadband Task Force (“BBTF”) Report are unnecessary for the purposes of interoperability.¹² For example, the NPSTC BBTF Report lists a number of “Desired Applications.”¹³ Although each of these may have value to some public safety users, none of these applications are truly required for interoperability, and thus should not be mandated by the Commission. Moreover, in some cases, such as with Commercial Mobile Alert System support, these applications are not presently commercially available.

¹² See NPSTC BBTF Report at 62-65.

¹³ *Id.* at 64-65.

Not all public safety users may have the same application needs. Accordingly, application decisions should be made collaboratively by individual public safety agencies, their system designers and their Internet service providers (“ISPs”). Mandating specific applications will add costs and complexity while reducing public safety flexibility, without any concomitant benefits. To the extent that any application-based interoperability issues arise, these would be most properly addressed by the vendor community in response to the needs and preferences of their public safety customers.

B. Roaming

The ability to roam, both between public safety broadband networks and onto commercial networks, will be essential to the success of the nationwide public safety broadband network. As AT&T emphasized previously, the Commission should support public safety’s request for Congress to permit reallocation of the Upper 700 MHz D Block to public safety. The D Block spectrum will be essential to the future development of public safety broadband networks, and will be particularly crucial during times of high traffic when many public safety users from other areas may be roaming on a single local or regional network.¹⁴

AT&T applauds the FCC for facilitating roaming by adopting the NPSTC BBTF recommendation that 3GPP Band 14—encompassing both the 700 MHz public safety broadband spectrum and the Upper 700 MHz D Block—be supported by all public safety broadband devices.¹⁵ Once the 700 MHz networks are substantially deployed, compulsory Band 14 support, especially combined with a reallocation of the D Block to public safety, might provide

¹⁴ See Section II.F. *infra*

¹⁵ *Waiver Order* at 17, ¶ 47; see also *NPSTC BBTF Report* at 19 (Section 6.3.1.5, “Devices”).

sufficient spectrum access to support robust mobile broadband services for a large number of public safety users, even while roaming.

However, before 700 MHz networks are fully deployed, public safety devices will need to roam onto commercial networks. Although use of the LTE protocol is a necessary component of interoperability for the 700 MHz public safety networks, public safety users should not be limited to 700 MHz or other LTE networks in their roaming options. If voluntary arrangements and technologically feasible solutions can be developed to allow roaming onto other frequency bands or other air interfaces, these methods should be embraced. Public safety agencies should have the benefit of as wide a choice as possible for roaming partners, allowing them to select the most advantageous arrangements for their areas and users.

To that end, AT&T has argued that, at a minimum, devices operating on the public safety broadband network should initially support the 1900 MHz PCS band and the 850 MHz cellular band, as well as 3GPP Band 14, and be backwards compatible with 3G networks, to ensure that public safety users can roam onto existing commercial wireless networks when outside the coverage area of the 700 MHz networks.¹⁶ Devices with these capabilities will accommodate roaming across most of the United States and can be designed and produced with a minimum of additional complexity. While compatibility with other bands should be a choice that public safety network operators are free to make based on their individual situations and commercial partnerships, such compatibility would not necessarily serve the purposes of nationwide interoperability and therefore should not be mandated.

¹⁶ See Letter from Jim Bugel, Assistant Vice President, Federal Regulatory, AT&T Services, Inc. to Marlene H. Dortch, Secretary, Federal Communications Commission, PS Docket No. 06-229, WT Docket No. 06-150 (filed May 26, 2010); See also Reply Comments of AT&T, Inc., RM No. 11592 at 17 (filed April 30, 2010) (discussing public safety roaming onto commercial 850 MHz and 1900 MHz networks).

AT&T has discussed allowing public safety users to roam onto commercial networks in the context of a “leveraged network” model for constructing public safety broadband networks.¹⁷ The leveraged network model is based on enabling local and regional public safety agencies to work with private sector partners to acquire the infrastructure and services required to develop their services. The model is based upon giving public safety agencies maximum flexibility to leverage existing and planned commercial resources to assist them in creating the best network for their specific needs, subject to minimum conditions designed to ensure interoperability. Under this approach, a nationwide “network of networks” would ultimately emerge, allowing public safety users to enjoy nationwide roaming.

Public safety agencies may wish to arrange for roaming access onto existing commercial networks, either as a permanent supplement to their own networks or as an interim solution while the public safety network is still being deployed. However, there should be no mandate for roaming onto any commercial bands, including, if not reallocated to public safety, the D Block. Instead, roaming should be a freely negotiated aspect of the public safety agency’s agreement with a commercial provider. Such negotiation will ensure access and service quality to public safety, while also allowing commercial providers to predict and control traffic on their networks accurately.

Public safety roaming onto commercial networks does raise questions about the applicability of certain Commercial Mobile Radio Service (“CMRS”) obligations to public safety devices and to commercial network operators with respect to public safety users. For example,

¹⁷ See, e.g., Comments of AT&T, Inc., PS Docket 06-229 at 17-18 (filed Oct. 16, 2009) (“AT&T Leveraged Network Comments”).

the Commission should clarify whether E911 and Section 255 requirements¹⁸ apply to public safety devices that are capable of roaming onto commercial networks. AT&T cautions the Commission to keep in mind that adding unnecessary requirements will increase the cost and complexity of public safety devices and may slow deployments. Despite roaming onto commercial networks, public safety devices and users will be distinct from CMRS devices and users, and the public safety devices will not be offered to the general public. Although some of their features may be integrated into the commercial network, and thus will be automatically offered, the Commission should take efforts to maintain the maximum flexibility for public safety agencies and commercial network operators to resolve these issues through their negotiations, with a focus on the needs and resources of the parties.

C. Priority Access

The *Public Notice* seeks comment on the technical requirements and operational issues related to the provision of priority access for public safety broadband networks. Development of a priority access regime for public safety users within public safety networks should be done within the public safety community, which will have the best sense of the classes of users that require priority and in what order. Although the Commission and ERIC might usefully provide a forum for discussing these issues, ultimately these decisions should not be made by a federal regulator. Furthermore, the LTE standards for priority access are in development. When finalized, the LTE prioritization standards will likely be sufficient for use in the public safety scenario. For example, these standards will allow for the identification of different classes of

¹⁸ See, e.g., 47 C.F.R. § 20.18(b) (“CMRS providers subject to this section must transmit all wireless 911 calls without respect to their call validation process to a Public Safety Answering Point”); 47 U.S.C. § 255 (“A manufacturer of telecommunications equipment or customer premises equipment shall ensure that the equipment is designed, developed, and fabricated to be accessible to and usable by individuals with disabilities, if readily achievable”).

users and for distinguishing between different classes with respect to call-routing priority.¹⁹ This functionality is consistent with what would likely be required with respect to priority access within public safety broadband networks.

Upon adopting a priority access regime based upon the LTE standard, public safety should address governance issues, which will be essential to the successful and functional operation of the system. Although effective governance is critical to the success of the priority access scheme, the Commission should not mandate specific governance structures or require that these structures be developed prior to the priority access process. Consistent with maintaining public safety agency flexibility and allowing the local and regional public safety networks to act as laboratories for the nationwide network, the Commission should allow these issues to be resolved organically within the public safety community in consultation with its industry partners.

With respect to priority access over commercial networks, the Commission should be mindful that relying on existing standards-based approaches and efforts will provide the simplest, most reliable and most cost effective means of satisfying public safety needs. For example, the Wireless Priority Service (“WPS”) has successfully achieved priority access over commercial wireless networks through a voluntary program that was fully funded by the Federal government. This model should be adapted and applied in the public safety broadband context.²⁰

Looking forward, the Department of Homeland Security’s National Communications Service (“NCS”) is currently developing the Next Generation Network Government Emergency

¹⁹ See Letter from Michael McMenamin, Alcatel Lucent to Marlene H. Dortch, Secretary, Federal Communications Commission, PS Docket No. 06-229 at 19-24 (filed April 19, 2010) (describing priority access features of LTE, including access class barring).

²⁰ See National Communications System, Wireless Priority Service, <http://wps.ncs.gov/> (last visited June 3, 2010).

Telecommunications Service (“NGN GETS”) industry requirements. The NGN GETS protocols will ensure that prioritization of national security and emergency preparedness (“NS/EP”) communications is maintained as communications networks transition from circuit-switch to IP-based infrastructures. The Commission should involve the public safety community in this development process and also work to coordinate public safety’s priority access requirements with the NGN GETS efforts. Additionally, the Commission should work to ensure full Congressional funding for the NGN GETS development efforts.

D. System Characteristics, Interfaces and Testing

In the *Public Notice*, the Commission seeks comment on issues related to network identification, authentication, and system testing. In all cases, public safety broadband networks should, to the extent possible, be developed and operated in accordance with standards and recommendations, such as those developed by NIST, ATIS, 3GPP and other such organizations. With respect to system identifiers, the NPSTC BBTF Report identifies two alternatives for assignment of the Public Land Mobile Network IDs (“PLMN ID”) required by 3GPP standards—either a single PLMN ID would be shared by all public safety networks or individual PLMN IDs would be assigned for each regional public safety network.²¹ AT&T recommends the former approach. Use of a single system identifier by public safety broadband networks nationwide will best facilitate roaming among the regional public safety broadband networks and between these networks and commercial networks.

Any questions related to interfaces and testing should also be resolved through a standards-based approach that is rooted in the LTE protocol and 3GPP process. AT&T supports public safety efforts to work with ATIS, the U.S. 3GPP organizational partner, to ensure that

²¹ *NPSTC BBTF Report* at 15-16.

these aspects of the public safety broadband network are developed in a standards-based manner on a continuing basis, and to promote developments in the 3GPP standards that are consistent with public safety needs.

E. Security

In the *Waiver Order*, the Commission adopted the NPSTC BBTF recommendation that public safety broadband networks support the optional LTE security features specified in 3GPP TS 33.401 and the use of VPNs.²² However, the Emergency Response Interoperability Center (“ERIC”) was vested with the responsibility of selecting the security features for the operation of the network. The *Public Notice* seeks comment on which specific features should be selected in order to maximize network security.

The Commission should not place detailed mandates on the security features of the public safety broadband networks, beyond the requirement that public safety broadband networks employ the security features of LTE. The LTE standard includes sophisticated air link encryption that would support VPN or other encryption on the application layer, as public safety needs demand. Taking advantage of built-in LTE security functionalities provides economies of scale for public safety, and ensures that the security systems remain current through the regular upgrades and updates to LTE.

In performing its mission, ERIC should not seek to specify all of the individual security features that should or should not be deployed because, due to the fast-evolving nature of cyber threats, any security mandates would quickly become outdated. Like all network providers, public safety operators will need to remain flexible in responding to security threats and should

²² *Waiver Order* at 17, ¶ 47; see also *NPSTC BBTF Report* at 21 (Section 6.3.3, “Security”); 3rd Generation Partnership Project, *Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security Architecture (Release 8)*, 3GPP TS 33.401 v8.7.0 (2010).

not be hamstrung in their efforts by static prescriptive regulations. Instead, ERIC’s involvement in this issue should be limited to ensuring interoperability between public safety broadband networks, and should not limit public safety’s ability to take advantage of ongoing technological development in this area. More critically, a one-size-fits-all approach to network security would be inappropriate—for example, urban areas such as New York and Washington, DC would likely require more stringent security protocols and protections than a more rural area might require. Adopting a uniform set of network security requirements may therefore unnecessarily add complexity and costs to the network construction for more rural networks.

F. Performance, Reliability, Capacity and Coverage

Questions of network performance, reliability, capacity and coverage are best left to the discretion of the public safety broadband network operator, in cooperation with any industry partners. Provided certain minimum technical and operational conditions are met, these network characteristics are not interoperability issues. Determination of these network characteristics will be highly dependent upon the budgetary limitations and operational demands of the regional public safety agencies. Accordingly, public safety agencies should be free to design this aspect of their networks according to their specific situations, in cooperation with their industry partners.

AT&T believes public safety is best served by a “network of networks” approach in which public safety agencies can make customized decisions on a regional basis that are specifically responsive to their needs, but that still allow for the enjoyment of scale economies, and that preserve nationwide interoperability. As the demands of regional networks are likely to differ dramatically depending upon terrain, population, and other factors, any strict federal mandate on network performance characteristics is likely to be a poor fit for some situations, and

might make some local or regional systems unfeasibly costly or complex. Moreover, as public safety agencies may attempt to leverage existing commercial infrastructure, particularly before their networks are fully constructed or through a network sharing agreement, detailed network performance characteristics may limit their options for commercial partners.

The most significant step that the Commission can take towards ensuring a consistently high level of network performance, reliability, capacity and coverage across all public safety broadband networks is to support the reallocation of the Upper 700 MHz D Block to public safety. The additional 10 MHz of paired spectrum that would be gained through a D Block allocation may be necessary to ensure reliable operation of the public safety broadband network in the long term.²³ With reallocation of the D Block, public safety broadband networks would provide higher peak data rates and increased overall network throughput, remain in the control of public safety, and operate with a single network infrastructure. Thus, allocation of the full 20 MHz provides the best “bang for the buck” for public safety, as it offers true broadband and multimedia functionality with the capacity for future growth and the greatest cost efficiencies.

G. Nationwide Core

The *Public Notice* seeks comment on the advisability of requiring a single nationwide core to which all the individual public safety broadband networks must connect. Although the *Public Notice* does not make clear what form a nationwide core would take, AT&T urges the Commission not to place such a requirement on the public safety broadband networks. Allowing

²³ See, e.g., Letter from Jim Bugel, AT&T Services, Inc. to Marlene H. Dortch, Secretary, Federal Communications Commission, WT Docket No. 06-150, PS Docket No. 06-229, GN Docket Nos. 09-47, 09-51, 09-137 (filed Jan. 21, 2010) (“AT&T Jan. 21, 2010 Letter”); Letter from Jim Bugel, AT&T Services, Inc. to Marlene H. Dortch, Secretary, Federal Communications Commission, WT Docket No. 06-150, PS Docket No. 06-229 (filed Dec. 18, 2009) (“AT&T Dec. 18, 2009 Letter”); Comments of AT&T, Inc., GN Docket Nos. 09-47, 09-51, 09-137, PS Docket Nos. 06-229, 07-100, 07-114, WT Docket No. 06-150, CC Docket No. 94-102, WC Docket No. 05-196 at 6-7 (filed Nov. 12, 2009) (“AT&T NBP PN #8 Comments”); AT&T Leveraged Network Comments at 12-14.

decisions of network design and operation to be made regionally will enable the development of public safety networks that are more responsive to the needs and resources of the regions the networks are designed to serve. Indeed, interconnection can be achieved most efficiently by leveraging regional commercial networks and databases that are already in place.

Adopting a nationwide core is likely to delay public safety broadband deployments that are otherwise ready to begin, and to restrict the operational flexibility of others. Questions of who is responsible for building, maintaining and financing the core, the basic capabilities and requirements of the core, and numerous challenges in coordination between multiple jurisdictions would likely have to be resolved before construction could begin on any regional public safety broadband network. Furthermore, depending upon the functionality of the core, it could limit the design flexibility that will be essential to enabling local and regional public safety agencies to develop on a timely basis broadband networks that meet their budgetary and operational needs.

As AT&T has expressed above and elsewhere,²⁴ public safety broadband needs would most quickly and efficiently be served through the development of regional, fully interoperable broadband networks, as opposed to a single nationwide network. This “network of networks” approach permits those localities and regions with the financial and other resources to immediately begin development of public safety broadband networks, allowing them to form a backbone on which other interoperable networks can be based, and bringing down construction and device costs for others.²⁵ This approach also permits experimentation with technology and

²⁴ See, e.g., AT&T Leveraged Network Comments at 5-7; AT&T Dec. 18, 2009 Letter at 4-5; AT&T Jan. 21, 2010 Letter at 4.

²⁵ See AT&T Leveraged Network Comments at 5-7.

procedures among the first deployed networks that will assist in the development of best practices for those that will come later.

Regional public safety broadband networks are a logical choice from a practical perspective as well. Public safety response is inherently a regional phenomenon insofar as emergencies tend to be geographically localized. Regional networks provide the best balance between taking advantage of economies of scale and making networks directly responsive and useful to local needs. Regions are likely to share certain environmental and other characteristics related to network development and will also have sufficient group buying power to effectively negotiate lower prices. Interoperability is required to ensure that, in the rare instances where public safety cooperation across regions is required, it can be sustained. The required use of the LTE protocol and the availability of a handful of basic functionalities, such as Internet access, will provide sufficient technical interoperability.

To facilitate roaming and interconnection between the public safety networks, AT&T recommends that regional public safety network providers work with private sector service providers to leverage existing commercial solutions. For roaming and interconnection to work seamlessly, there is a critical need for a specialized database to be created and maintained for the national public safety network. However, this database need not be maintained at the national level. Indeed, there may very well be opportunities for public safety to work cooperatively with commercial providers to leverage existing commercial routing/interconnection database systems. These solutions could be adapted for public safety use and would save public safety the time and expense that would be required to develop, implement and maintain a specialized nationwide core simply to accommodate these functions.

H. Network Operations, Administration and Maintenance (OA&M)

The *Public Notice* seeks comment on whether it would serve the goals of interoperability and consistency for the Commission to require the implementation of any specific models for network operations, administration and maintenance (OA&M).²⁶ The *Waiver Order* was appropriately silent on this point. The NPSTC BBTF report assumed that regional operators would maintain control over network construction and establish their own internal protocols governing the use of their system.²⁷ The Commission should follow this recommendation and defer to the regional public safety network operators' judgment on matters of OA&M. These decisions are not interoperability-related and are highly likely to be influenced by staffing, budgetary constraints and other concerns that are best addressed on a local, state or regional level. Although the Commission and the ERIC might usefully provide recommendations and act as a forum for standardizations of practices, no federal mandates should be adopted.

I. Governance

The *Public Notice* seeks comment on how to ensure a governance structure that promotes interoperability in public safety broadband networks nationwide. The NPSTC BBTF report recommendations propose regional governance through spectrum leases from the Public Safety Broadband Licensee.²⁸ Under the NPSTC BBTF proposal, a Regional Operator Advisory Group could be formed consisting of a representative from each regional operator and the PSST to conduct follow-on work and to resolve any issues that arise during network deployment and

²⁶ *Public Notice* at 3.

²⁷ *See NPST BBTF Report* at 23-24 (Section 8.8, "Operating Protocols").

²⁸ *See id.* at 21-22 (Section 6.4, "Governance").

operation.²⁹ This approach will best allow regional governance to be contained at a level that is responsive to local concerns, while also ensuring that national or multi-regional issues related to interoperability or future network development are made in a responsible and representative way. The Commission should express support for the NPSTC BBTF model, which will allow maximum flexibility with continued interoperability, while providing no federal mandates. As the public safety broadband networks will ultimately be most effectively and efficiently run if public safety is in control, the Commission should not dictate a specific governance model. Similarly to OA&M,³⁰ the Commission and the ERIC can best facilitate the development of an appropriate governance structure by acting as a forum for discussion and standardization and by offering recommendations to be implemented at the discretion of the public safety community.

III. OUT-OF-BAND EMISSIONS

In the *Waiver Order*, it was suggested that an out-of-band emission (“OOBE”) limit of $43 + 10 \log P$ be adopted for the public safety broadband systems.³¹ Current OOBE limits for public safety are inconsistent, varying dramatically based on whether they were intended to protect the public safety broadband network from the D Block or the public safety narrowband channels from the adjacent commercial 700 MHz blocks.³² AT&T believes that the best way to alleviate the OOBE concerns between commercial and public safety entities is to reallocate the 700 MHz D Block for public safety use. Reallocation would eliminate any concerns about interference between the D Block and public safety broadband spectrum. However, absent such a reallocation, AT&T suggests that the Commission apply the general $43 + 10 \log P$ OOBE

²⁹ *Id.* at 11 (Section 6.1.1, “Regional Operator Advisory Group”).

³⁰ *See* Section II.H., *supra*.

³¹ *See Waiver Order* at 15, ¶ 44.

³² *See* 47 C.F.R. § 90.543.

limit.³³ Such an approach would be consistent with past precedent for OOB limits and would allow public safety the flexibility to implement broadband networks.

In addition, AT&T suggests that the Commission review the entire OOB framework for the 700 MHz band, especially as it applies to public safety systems. In particular, there appear to be inconsistencies in OOB protections between narrowband and broadband systems. Moreover, as the OOB limits have been adopted over time and in different Commission proceedings, AT&T believes that a full investigation and discussion of OOB limits by the Commission for public safety spectrum would be of great benefit. Through this effort, public safety (and adjacent band commercial licensees) will be better positioned to understand the requirements for OOB limits in the 700 MHz band.

IV. EQUIPMENT CERTIFICATION

In the *Waiver Order*, the Commission recognized that due to the unique nature and accelerated deployment timing of the regional public safety broadband networks, there will not likely be certified equipment available for these networks before build-out begins.³⁴ Accordingly, the Commission waived its equipment certification rules, provided that the waiver recipients and their manufacturers conform with the requirements of the LTE standard pending finalization of technical rules.³⁵ In the *Public Notice*, the Commission seeks comment on what equipment certification requirements should be placed upon public safety broadband devices,

³³ The Commission should still retain the appropriately stringent OOB limits designed to protect narrowband public safety operations. *See* 47 C.F.R. § 90.543(d).

³⁴ *Waiver Order* at n.88.

³⁵ *Id.*

and how to address the continued development of the LTE standard and its impact on interoperability.³⁶

LTE has been conceived as an ongoing developmental process that will include backwards compatibility at every stage of future development. The Commission appropriately conditioned the waivers on device compliance with the LTE standard. In any final rules that are adopted, the Commission should strive to ensure that the technical parameters of the 3GPP Release 8 LTE specifications are embraced by public safety broadband devices. To the extent that these requirements are not met, or that public safety broadband devices have requirements differing from those provided through LTE, public safety will lose the benefits of economies of scale and scope as their devices will no longer be able to fully utilize the chipsets, antennas, and other equipment developed for commercial networks. Moreover, noncompliance with the LTE standard could also jeopardize the ability of public safety users to roam on commercial networks.

With respect to the ongoing development of the LTE standard, the Commission's final rules must provide sufficient flexibility for public safety to take full advantage of future releases of LTE. Due to the backwards compatibility inherent in the LTE development process, networks deploying future releases of LTE will support roaming by devices operating on earlier releases, and vice versa. Thus, provided the Commission's rules maintain a standards-based approach, interoperability between networks operating on differing LTE releases should not be problematic. To have an influence on the ongoing evolution of the LTE standard, public safety should work closely with ATIS to ensure that its views and needs are represented through the 3GPP development process. As the U.S. organizational partner in 3GPP, membership in ATIS

³⁶ *Public Notice* at 4-5.

represents the appropriate forum for public safety to participate in the continuing development of the standard.

Ultimately, the Commission should require the same equipment testing and certification processes as are currently applied to CMRS devices. It is expected that most commercial LTE devices will undergo Commission and industry-recognized certification testing based on 3GPP and Open Mobile Alliance (OMA) standards, such as that provided by the PTCRB or the Global Certification Forum (GCF), prior to being authorized for operation on most commercial LTE networks. The Commission and industry testing processes will be equally effective in demonstrating safe operation and interoperability for public safety devices and networks, provided that these devices and networks are designed in compliance with commercially used standards, as expected. AT&T notes again that, to the extent Commission testing or certification for CMRS devices presupposes any uniquely CMRS obligations (such as E911 or Section 255 compliance), these requirements should be waived with respect to public safety devices.

V. CONCLUSION

In the *Waiver Order*, the Commission generally struck an appropriate balance between ensuring interoperability of the regional public safety broadband networks and preserving the flexibility of public safety entities to experiment and develop the best network to meet their specific needs. In crafting final rules to govern public safety wireless broadband systems nationwide, the Commission should strive to set only the minimum technical and operational requirements needed for interoperability. To the extent that the Commission attempts to dictate the specific technical or operational characteristics of public safety broadband networks, it risks limiting the flexibility of the regional network operators and the feasibility of the overall project. At every step, the Commission should promote LTE standards-based specifications and

commercially accepted practices as the best path to ensuring the development of a robust and interoperable nationwide public safety broadband network that will remain effective and vital far into the future.

Respectfully submitted,

AT&T Inc.

A handwritten signature in black ink, appearing to read "Robert Vitanza", with a long horizontal flourish extending to the right.

By:

Robert Vitanza
Gary L. Phillips
Paul K. Mancini
AT&T Inc.
1120 20th Street, N.W.
Washington, DC 20036
(202) 457-3076
Counsel for AT&T Inc.

July 19, 2010