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

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

COMMENTS OF ALCATEL-LUCENT

Michael McMenamin
Jeffrey Marks

1100 New York Avenue, NW, Suite 640
Washington, D. C. 20005
(202) 316-5916

April 11, 2011

TABLE OF CONTENTS

SUMMARY

Alcatel-Lucent welcomes this opportunity to participate in this proceeding, which will have a profound impact on the future of public safety broadband deployments. The Federal Communications Commission's ("FCC/Commission") adoption of Long Term Evolution ("LTE") as the common standard technology for the 700 MHz public safety broadband block was a major step towards creating the interoperable broadband network that Congress and the 9/11 Commission envisioned. No less important is the need for this nation's first responders to roam across public safety and commercial partners' networks. This proceeding lays the foundation for future public safety deployments and moves us ever so much closer to the long overdue nationwide public safety network.

As the technology of choice by United States and global service providers, LTE technology and equipment will continue to evolve providing for better spectral efficiencies, more features while maintaining backward compatibility. Over time, network equipment costs will decrease because of public safety's ability to leverage economies of scale.

At the outset, there is a need for a governance model or structure in order to facilitate the construction, operation and maintenance of the nationwide public safety network. Governance models, as they apply to shared public safety networks are not new, as reflected in some of the legacy narrowband State networks. However, the nationwide broadband model should address funding and oversee the requirements on architecture, interfaces, and network evolution before an appropriate network architecture can be finalized. Network architecture can range from a single geographically distributed core with a single operator, to a large number of networks each individually owned and operated. Any approach should account for the near term deployments that are part of the Broadband Stimulus program.

With respect to network architecture, there are four main alternatives that should be considered: a single geo-redundant core network (7-10 sites) with a single PLMN id ("Public Land Mobile Network Identifier") operated by a single operator; a Network of networks, with a single PLMN id for all networks using an HSS routing and charging entity to coordinate between the individual networks; a small number of networks (~10) each with their own PLMN id; and a network per state/major city each with their own PLMN id (~50), and using the nationwide umbrella PLMN to facilitate roaming. We have concluded that any one of the above alternatives will work.

In addition, we seek an open consensus standards process, which is essential towards creating competition. We recommend that the Commission consider the OMB Circular No. A–119 consensus standard process that will provide public safety and industry partners a major role in its implementation. We believe this process should be used to define in sufficient detail all capabilities that are considered critical to nationwide interoperability, including devices, network infrastructure and architecture, key applications, and application programming interfaces (APIs) enabling access to critical network functions like Quality of Service ("QoS") and priority access.

In regards to nationwide framework for QoS and priority access, we believe that governance rules should be defined across all public safety jurisdictions for use of LTE's Allocation and Retention Priority ("ARP") and QoS Class Identifier ("QCI") to facilitate priority access services for public safety networks.

As for out-of band emissions, we support the Commission's current specification of $43 + 10 \log_{10}P$ as the Out-of-Band Emissions limit for operations in the public safety broadband block.

In the case of applications, those specified by the NPSTC Broadband Task Force Report ("NPSTC BBTF") should not be in the scope of the initial stage of the national network, except for the Virtual Private Network access, the status or information "homepage," and the location based data capability, which will first require further definition and possibly standards enhancements. In regards to the interconnection with legacy public safety LMR networks, we recommend the use of gateways between legacy LMR networks and users on the public safety broadband network and standardized interfaces between the LTE Push-To-Talk ("PTT") client and the PTT server in the LTE network.

As for performance, reliability, capacity and coverage of the public safety network, we disagree with the Commission's suggestion of establishing design edge rate requirements. The suggested rates are atypical of commercial network designs, which generally aim for lower edge rates. By the same token, local jurisdictions know best their operations, needs and hence are in the best position to dictate coverage requirements. In addition, the Commission should adopt new definitions for spectral efficiency, such as for system spectral throughput rather than the usual bandwidth efficiency. Finally, the FCC should not regulate the type of 3GPP standard mechanism employed to minimize cell border interference or improve cell edge throughputs.

Roaming on the public safety broadband network should be covered by existing 3GPP Rel. 8 standards where end-user devices will support the appropriate frequency bands. In addition, the establishment of roaming and handoff among neighboring public safety networks will require appropriate security mechanisms be put in place. Handoffs although complicated, will benefit from performance enhancements techniques that are part of 3GPP Rel. 9 specifications.

Further, we support the requirement of conformance testing for user devices that will be allowed to operate on the public safety broadband network using the well established PTCRB approach. We propose that due to complexity of LTE infrastructure, infrastructure vendor self-certification of network elements be permitted, and that these manufacturers submit to TL9000 certification, assuring high quality process and well documented and traceable requirements from feature request through delivery, with external audit of the company's compliance to their processes. We envision leveraging the National Institute of Standards and Technology ("NIST") Public Safety Communications Research ("PSCR") environment to support first office application

testing of public safety specific features that are incremental to those tested in normal commercial operator environments. In regards to interoperability testing, Alcatel-Lucent recommends that processes in place for interoperability testing on commercial LTE networks should be leveraged. Furthermore, interoperability across interfaces should be required on those interfaces that will impact roaming and device/application interoperability with the network as outlined in paragraph 110 of this proceeding.

Alcatel-Lucent supports the use of the public safety network by federal users and critical infrastructure. By enabling their access to the 700 MHz public safety broadband spectrum it will enhance coordination during emergencies and, importantly, spread the costs of building the public safety broadband network among multiple stakeholders. Finally, we disagree with the Commission's tentative conclusion that fixed mobile services should only operate in the 700 MHz band on an ancillary basis.

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

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

To: The Commission

COMMENTS OF ALCATEL-LUCENT

Alcatel-Lucent welcomes this opportunity to respond to the Federal Communications Commission ("FCC/Commission") Third Report and Order and Fourth Further Notice of Proposed Rulemaking ("*Fourth Further Notice*") seeking comment on additional requirements to further promote and enable nationwide interoperability among public safety broadband networks operating in the 700 MHz band.[1]

The Commission's choice of Long Term Evolution ("LTE") as the common air interface for public safety is the initial first step towards creating an interoperable broadband network that Congress and the 9/11 Commission envisioned. No less important is the need for this nation's first responders to have interoperability with the

[1] *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, ¶ 15 (rel. Jan. 26, 2011) ("*Fourth Further Notice*").

ability to seamlessly roam across public safety networks, as well as those of their commercial partners. This proceeding lays the foundation for future public safety deployments and moves us ever so closer to a nationwide public safety network.

I. AT THE OUTSET, A GOVERNANCE MODEL IS NEEDED TO APPROPRIATELY ADDRESS MANY OF THE ISSUES IN THIS PROCEEDING

Over the last few years, the Commission has taken significant steps to advance nationwide interoperable public safety broadband communications. At this juncture, the next most significant step towards making the public safety broadband network ("PSBN") a reality is the formation of a public safety governance model. The governance model should establish how the construction, operation and maintenance of the nationwide public safety network will be funded and oversee the substantive requirements on architecture, interfaces, network evolution and other topics in the *Fourth Further Notice* are established for the nationwide network. A governance structure is needed for a variety of purposes, including:

- providing common requirements and use cases for the nationwide network and updating these requirements and use cases as technology and mission-needs evolve;
- establishing a common architecture framework;
- establishing a process for ongoing testing and certification of user devices, network components and software;
- establishing a representative process to take into account the needs of the nearly 60,000 public safety agencies in the United States ("U.S.") in the development of requirements;
- clearly specifying the rights and responsibilities of all entities participating in construction, maintenance and operations of the nationwide network
- determining how the costs for operating and maintaining the network should be shared among entities;
- establishing procedures for resolving disputes among parties;
- establishing coordinated network rollout plans to allow multiple states, for example, to share network components and transmission facilities;
- establishing governance procedures to ensure transparency;

- establishing service level agreements;
- monitoring and reporting of the service levels achieved;
- establishing roaming agreements; and
- establishing policies and critical parameters for sharing the network with secondary users.

We believe that the ensuing architecture for the nationwide public safety network will be influenced greatly by the governance model, which can range from a single geographically distributed core with a single operator, to a large number of networks each individually owned and operated.

II. ALCATEL-LUCENT GENERALLY AGREES WITH THE COMMISSION'S CONCLUSION IN THE THIRD REPORT AND ORDER THAT CERTAIN RELEASE 8 LTE INTERFACES MUST BE SUPPORTED

To ensure interoperability requirements are met, Alcatel-Lucent agrees with the FCC that interface specifications should be required for interoperability. Based on the record in this proceeding, the FCC is requiring certain Rel. 8 LTE interfaces:

- Uu- LTE air interface
- S6a – Visited MME to Home HSS
- S8 – Visited SGW to Home PGW
- S9 – Visited PCRF to Home PCRF for dynamic policy arbitration
- S10 – MME to MME support for Category 1 handover support
- X2 – eNodeB to eNodeB
- S1-u – beween eNodeB and SGW
- S1-MME – between eNodeB and MME
- S5 – between SGW and PGW
- S6a – between MME and HSS
- S11 – between MME and SGW
- SGi – between PGW and external PDN
- Gx – between PGW and PCRF (for QoS policy, filter policy and charging rules)

- Rx – between PCRF and AF located in a PDN
- Gy/Gz – online/offline charging interfaces

We agree that the first four of these interfaces are important for achieving interoperability when roaming across networks, while the rest are necessary to ensure multi-vendor interoperability for equipment and devices operated on the same network with one exception. However, the purpose for online charging in a public safety network is unclear to us. Consequently, Alcatel-Lucent does not recommend including the Gy interface.

Finally, given the uncertainty of the deployment strategy of the public safety network, we emphasize the need for requiring multi-vendor interoperability. We contend that this is critical to the success of the public safety network, even if initially the networks will be single vendor.

III. THERE IS A NEED FOR CERTAIN FCC-MANDATED TECHNICAL RULES TO ENABLE BUILD-OUT OF THE PSBN, BUT IN MANY INSTANCES A GOVERNANCE MODEL IS NEEDED FIRST

1. Architecture

Alcatel-Lucent has carefully evaluated the various architecture proposals suggested for the nationwide public safety network. We believe that there are four main alternatives that should be considered, each with multiple sub-options:

- Single geo-redundant core network (7-10 sites) with a single PLMN ids ("Public Land Mobile Network Identifier") operated by a single operator with an approved, IOT tested set of eNodeB, SGWs, and PGWs from various vendors;
- Network of networks, using a single PLMN for all networks using an HSS routing and charging entity to coordinate between the individual networks. The routing entity should include a Diameter Routing Agent ("DRA"), which can be used for all diameter interfaces, whereas a Subscriber Locator Function ("SLA") is only used for the HSS. Note this could result in a large number of individual networks which could increase the cost to operate these networks significantly;
- A small number of networks (~10) each with their own PLMN; and

- A network per state/major city each with their own PLMN id (~50), and using the nationwide umbrella PLMN id for roaming. Note this requires support for the Multi-Operator Core Network (MOCN) and the Gateway Core Network (GWCN) feature functionality as defined by 3GPP.

Alcatel-Lucent has concluded that any one of the above alternatives will work. We believe, however, that a decision on the governance model is needed before a network architecture is chosen, ensuring a common network architecture for the nationwide network.

If a network architecture using multiple PLMN ids is chosen, Alcatel-Lucent believes that support for home-routed and local breakout traffic is required. Home-routed APN ("Access Point Name") is needed to access information in the home network, including access to the NCIC database. Roaming using local breakout allows services from the home network, the visited network, or a combination of the two. An example is an internet APN that uses local breakout and avoids backhaul to the home network first, while reducing delay. Local breakout can also be leveraged to provide access to a home page/access portal when users visit other jurisdictions.

Moreover, network interconnection depends on the governance model, whether it be a single or multiple networks with single or multiple PLMN ids. In a single core with a single PLMN interconnection, it will likely be managed at the national level and an IPX/clearinghouse may be used to connect to commercial networks. Similarly pairwise roaming agreements with commercial operators may be practical alternative. Through the use of other solutions, the ability to interconnect would require a nationwide backbone to be put in place for public safety or the ability for each individual network to connect to other public safety and commercial networks through an IPX/clearinghouse. In the latter case, public safety networks may also choose to directly connect with one

another, which in certain cases would improve handover times or reduce interconnection costs, especially for neighboring entities. Finally, we believe the introduction of a nationwide backbone needs careful consideration, including consideration of equipment costs, as well as operations/leasing costs.

2. Open standards

Alcatel-Lucent recommends an open standards process, which is essential towards creating both innovation and competition. Public safety broadband networks will be advantaged with respect to cost and innovation by leveraging commercial standards that will provide the foundation for the national network. Over time, industry consensus standards will evolve, such as those specified by OMB Circular No. A - 119, providing public safety and industry partners a major role in its implementation that will allow for the ability to have open, standards based broadband public safety networks deployed more rapidly when compared to P25.[2] Also, LTE networks being deployed by service providers in the U.S. and globally are inherently multi-vendor because of the standardization process of 3GPP.

Competition, however, is not itself sufficient to ensure interoperability. For instance, the delays in specifying the P25 ISSI specifications yielded limited interoperability between systems that resulted in one dominant vendor in the U.S. marketplace. In fact, it took more than 20 years for two P25 systems to simply talk to each other, while commercial systems have gone through roughly three wireless technology generations in the same period**.** The reliance on an open standard for LTE and the required inter-vendor equipment testing will ensure equipment interoperability.

[2] *See* Office of Management and Budget, Circular A-119, Federal Participation in the Development and Use of Voluntary Standards (Feb. 10, 1998) *available at* http://www.whitehouse.gov/omb/circulars_a119/.

Open standards at all layers of the network enable different vendors to affordably participate in the ecosystem more readily without having to provide a total solution.

Alcatel-Lucent believes that adoption of standards via an open consensus process that includes participation by public safety and vendors and the use of cross-licensing practices is essential in ensuring increased competitiveness in the public safety marketplace. LTE, today, is being rolled-out commercially and has cross licensing practices that are creating a competitive environment.

Moreover, without 3GPP standards, interoperability will be jeopardized, possibly not as much in initial single-vendor networks, but certainly longer-term, as networks from different jurisdictions have to inter-work. This, however, does not preclude "proprietary" value-added services from vendors to differentiate their offerings as long as they do not add additional parameters or change the meaning of existing parameters on the 3GPP defined interfaces, which would affect interoperability. In fact, the 3GPP standards today leave room for innovation by only standardizing aspects that effect functionality/interoperability. For example, the way the policy engine in the Policy and Charging Resource Function ("PCRF") works the scheduling of the algorithm in the eNodeB is not standardized and allows vendor differentiation without affecting interoperability.

Finally, a governance and funding model needs to be defined before a decision can be made whether rules and/or timeframes should be put in place to upgrade to later 3GPP releases. Clearly, later 3GPP releases are introducing functionality desired by public safety, such as enhanced Multimedia Broadcast Multicast Service ("eMBMS"), which is viewed as a critical feature to support large talk groups. Moreover, the

governance model must address how 3GPP future releases will be built into the network in order to ensure technological consistency throughout the network.

3. Technology Platform and System Interfaces

The Commission seeks comment on support for Proxy Mobile IP ("PMIP") for certain LTE interfaces. In order to maximize interoperability with commercial networks, Alcatel-Lucent recommends use of GPRS Tunneling Protocol ("GTP") only for the S5/S8 interface, since this is what all commercial LTE vendors are using. Support for PMIP is required to interconnect the Home Service Gateway ("HSGW") with the Packet Data Network Gateway ("PDN-GW") via the S2a interface, and to interconnect the enhanced Packet Data Gateway ("ePDG") with the PDN-GW via the S2b interface for network-based mobility with Wi-Fi networks. It is unclear, however, whether these inter-Radio Access Technology ("inter-RAT") roaming and resulting handoff mechanisms will be used for the PSBN. Thus, PMIP should not be dealt with in the scope for this proceeding.

In order to support IPv4 and IPv6, Alcatel-Lucent also recommends support for dual stack in all elements of the LTE network with the exception of the eNodeB. Supporting dual stack in these elements allows for a very smooth migration from IPv4 to IPv6 when the desired enablement is needed in the core, and then switching the eNodeBs one-by-one from IPv4 to IPv6.

4. Nationwide Framework for QoS and Priority Access

Alcatel-Lucent recommends that governance rules should be defined across all public safety jurisdictions for use of LTE's Allocation and Retention Priority ("ARP") and QoS Class Identifier ("QCI") to facilitate priority access services for public safety networks. The definition should include the treatment of public safety users roaming onto another jurisdiction's network and the need for commercial service providers to agree on a recommended treatment for ARP and QCI when roaming from public safety networks into commercial networks. The priority access levels for when an outside public safety user roams into the commercial and/or public safety jurisdiction network should be defined. The below figure provides an example of a potential scheme.

Priority	User groups		GBR Bearer		Non-GBR Bearer	
			Can Pre-empt	Vulnerable	Can Pre-empt	Vulnerable
1	1st responder at home (A)		Yes	No	Yes	No
2	1st responder at home (B)		Yes	No	Yes	No
3	1st responder at home (C)		Yes	No	Yes	No
4	1st responder at home (D)	1st responder visiting (A)	Yes	No	Yes	No
5	1st responder at home (E)	1st responder visiting (B)	Yes	No	Yes	No
6	PS support at home (A)	1st responder visiting (C)	Yes	No	No	Yes
7	PS support at home (B)	1st responder visiting (D)	Yes	No	No	Yes
8	PS support at home (C)	1st responder visiting (E)	Yes	No	No	Yes
9	PS support at home (D)	PS support visiting (A)	Yes	No	No	Yes
10	PS other (A)	PS support visiting (B)	No	Yes	No	Yes
11	PS other (B)	PS support visiting (C)	No	Yes	No	Yes
12	PS other (C)	PS support visiting (D)	No	Yes	No	Yes
13	PS other (D)		No	Yes	No	Yes
14	Commercial user		No	No	No	No
15	Commercial user		No	No	No	No

As the figure shows, the individual jurisdictions still have the freedom to appropriately assign priority access levels to the outside roamers use of the network. The priority access mechanism can be in effect at all times. In normal situations it is expected that

sufficient capacity will be available in a given eNodeB to not trigger pre-emption. We do, however, anticipate the need to modify the priority scheme during certain emergencies, so that appropriate public safety personnel will have access to the needed network resources.

Further, we see limited need to modify QCI values for specific traffic, primarily associated with non-Guaranteed Bit rate traffic with QCI values of 6, 8, and 9 that have the same performance characteristics, but result in a different priority handling in the eNodeB and backhaul. It would, however, allow for different priority levels for non-GBR traffic. There may also be a need to limit the maximum bit rate a user may get during times of congestion.

Moreover, governance rules should define the methodology within the 3GPP standards framework for how public safety applications interact with the LTE PCRF and PDN-GW/Serving Gateway, including roaming implications, so that applications may be developed and enhanced to support QoS and priority access in a timely manner. Alcatel-Lucent believes that standards are available in Rel. 8 to support this functionality.

Finally, we believe that the priority access schemes in this context will not be compatible with those deployed over commercial networks, since commercial providers have different network priorities than public safety and are unlikely to accept priority schemes that are desired by public safety. For example, commercial providers could provide a much smaller number of ARP values for public safety use, allowing them to use ARP for commercial uses as well. The commercial provider, however, would not typically permit pre-empting consumer customers. Moreover, we recommend encouraging compatibility with NGN-GETS for government users.

5. Out-of-Band Emissions

Alcatel-Lucent supports the Commission's current specification of $43 + 10 \log_{10}P$ as the Out-of-Band Emissions ("OOBE") limit for operations in the public safety broadband block. The risk for adjacent interference, which is always present in wireless networks, can be managed, but it requires clarity from public safety and/or the FCC. For instance, in the public safety context an important point to consider is whether reduction (due to interference) in data throughput is more important than data coverage. Any attempt at making OOBE limits more stringent or introduce guard-bands will delay the availability of public safety equipment, devices, and in the network deployment.

6. Applications

Alcatel-Lucent recommends that the desired applications specified in the NPSTC Broadband Task Force Report ("NPSTC BBTF Report")[3] should not be entirely considered for the initial network requirements. Of the applications identified by the NPSTC BBTF Report, we believe that Virtual Private Network ("VPN") access, the status or information "homepage," and the location based data capability require further definition to assure interoperability, and these interoperability specifications should be clearly defined for the initial focus for the broadband network. We recommend the architecture forum proposed as part of the governance structure should be used to define the architecture for these three items. If required, the FCC can subsequently capture the recommendations of this forum in a rulemaking.

[3] *See* National Public Safety Telecommunications Council, 700 MHz Public Safety Broadband Task Force Report and Recommendations (2009), *available at* http://www.npstc.org/documents/700_MHz_BBTF_Final_Report_0090904_v1_1.pdf.

As for the SMS/MMS messaging application, we believe all that is required is to clarify that this application should follow the 3GPP TS 23.204 and related standards for SMS/MMS over IP. For the remaining NPSTC applications, we do not believe further rulemaking is required. In addition, beyond the above items, we believe the FCC can promote application interoperability by focusing on enabling applications through the use of standards-based Application Programming Interfaces ("APIs") such as the ones defined in GSM Association's OneAPI, as opposed to identifying specific applications. Focusing on APIs will enable an ecosystem of public safety applications. This is another area that we believe that the architecture forum can provide guidance.

7. Interconnection with legacy public safety/LMR networks:

Alcatel-Lucent recommends the use of gateways between legacy land mobile radio ("LMR") networks and LMR users on the public safety broadband networks, leveraging the Inter-RF Subsystem Interface ("ISSI") interface as defined by Telecommunications Industry Association. This will allow full-feature functionality on LTE LMR-enabled devices. We demonstrated this capability at the APCO Conference in Houston, Texas in August 2010. We expect this capability to be available for non-mission critical Push-To-Talk ("PTT") in the 2012/2013 timeframe, subject to timely standardization.

In order to enable the broadest ecosystem for devices as well as PTT servers for LTE, it is critical to standardize the interface between the LTE LMR user equipment ("UE") and the PTT server in LTE, as well as an IP-based interface between LTE PTT servers. The latter will provide a seamless interworking in the mission-critical PTT functionality and allow for migration to LTE without a continued need for interworking gateways. We anticipate that this will take approximately five years, as a number of

technical issues will need to be addressed and standardized, most notably talk-round. In addition, as the PTT functionality migrates to LTE it is expected to use the industry standard Voice over LTE ("VoLTE") as defined by GSMA for one-on-one conversations instead of user-to-user PTT, except in those instances where one of the parties is on a LMR network. Moreover, the same VoLTE capability will also provide interworking from LTE devices to the PSTN.

8. Security and Encryption:

Alcatel-Lucent does not believe public safety LTE networks should implement all optional feature requirements in 3GPP TS 33.401, but instead should follow the guidelines specified in NPSTC's BBTF Report. As per the NPSTC report, the Radio Resource Control ("RRC – TS 36.311") protocol layer may optionally implement LTE signaling layer security features. The Network Access Stratum ("NAS – TS 24.301") protocol layer may optionally implement EPC signaling layer security features. The Packet Data Convergence Sub layer ("PDCP – TS 36.323") protocol layer may optionally implement user data plane security features. For public safety LTE networks, Alcatel-Lucent recommends these specific optional security layer features in 3GPP TS 33.401 be implemented. We also recommend all the Authentication and Key Agreement ("AKA") procedures in sections 6, 7 and 8 from TS 33.401 be implemented to support authentication and key management, handover, and other relevant security applications.

While 3GPP TS33.401 refers to 33.210 and 33.310, which allow for a multitude of algorithms, *e.g*. Internet Key Exchange version 1 and 2 ("IKEv1", "IKEv2"). Alcatel-Lucent suggests following 3GPP TS 33.401 recommendation: IPSec Encapsulating Security Payload with IKEv2, certificates and tunnel mode with Security Gateway.

9. Performance, Reliability, Capacity and Coverage

While there is a need to leverage the capabilities of broadband technologies and meet applications requirements such as high cell edge data rates, the associated implications on the overall cost of the network must be considered because large edge rates will typically require smaller inter-site distances. To suggest 768 Kbps and 256 Kbps edge rates is atypical of commercial network designs, although most commercial networks are focused on urban to semi-urban environments with an emphasis on meeting capacity needs rather than coverage. We contend that high edge rates is counter to the desire by jurisdictions to leverage their legacy "low data rate" LMR sites whose inter-site distance is generally larger than inter-site distances in a "higher data rate" LTE system. Moreover, assigning a loading factor is not relevant to the downlink since LTE designs will account for full use of the resource blocks to achieve a certain downlink rate based on the uplink maximum path loss.

In the end, interoperability is not synonymous with service availability. Two distinct contiguous radio systems built around different service edge criteria, with one network denser than the other, can still allow for interoperability. In that regard, we dissociate the extent of the service availability from the radio coverage perspective with interoperability the process enabling communications will be available.

There is the potential need for the Commission to adopt new definitions for spectral efficiency, such as for system spectral throughput rather than the usual bandwidth efficiency. The Commission, however, should not rule on the targeted bps/Hz, whether as an aggregate or edge throughput, since most figures vary from vendor to vendor because of the differences in their implementation of the radio resources

scheduler. In addition, there are limits to how much a particular technology can provide in a specific context *e.g.* standard techniques may be more applicable to higher frequency bands than for the 700 MHz band.

In regards to coverage needs, jurisdictions know best their coverage requirements. Traditionally, 95% outdoor area coverage reliability has been a common design figure for urban to less urban areas and 90% for rural areas. Higher objectives lead to a higher cell count, potentially higher cost, and lower objectives lead to a lower cell count and lower cost. Mandating a coverage reliability objective without accounting for available funding would not be a prudent approach, unless there is a common understanding that such a requirement will likely restrict the size of the service area. Likewise, we believe that a ruling on indoor network deployment would be premature, given that coverage of hard to reach areas is specific to each local jurisdiction.

Generally, agreements between a jurisdiction and a chosen infrastructure supplier determine the extent of the coverage that can be validated based on coverage testing. Hence, it is premature to mandate a timeline, like 30 days, to validate a particular coverage design irrespective of the size of the service area or the targeted metrics. Service area coverage gaps are typically remedied through agreed upon measures based on the network acceptance test plan.

Finally, Alcatel-Lucent does not believe that the FCC should regulate the type of mechanism employed to minimize cell border interference or improve cell edge throughputs. At this stage, geographical jurisdictional boundaries have not been set for the network. In a single-vendor approach measures will be taken to optimize the cell

border throughput and in multi-vendor network the vendors should be expected to work together on the best approach to achieve the same objective.

10. Network Operations, Administration and Maintenance

Alcatel-Lucent believes that Network Operations, Administration and Maintenance ("OA&M") is generally vendor specific and should not be subjected to specific requirements beyond the ones already defined by the various standards bodies, *e.g.* charging, call tracing. In addition, device management should follow the requirements as set forth in 3GPP and Open Mobile Alliance ("OMA") standards.

IV. DEFINING NETWORK CAPABILITIES FOR PUBLIC SAFETY ROAMING ON THE PSBN

Standards for handoff and roaming between public safety LTE networks as well as with commercial LTE networks can be covered by existing 3GPP Rel. 8 standards where end-user devices will support the appropriate frequency bands. Defining any additional roamer types (itinerant, interoperability, or response roamers) would be beyond the 3GPP standards, and it is unclear who would categorize each of the user groups. Thus, we recommend that individual jurisdictions be allowed to decide roaming on their networks once governance rules are completed that define the number of public safety networks and boundaries.

The establishment of roaming agreements will require appropriate security mechanisms among public safety networks that allow for roaming. Inter-RAT ("Radio Access Technologies") handoff to technologies such as GSM, UMTS, HSPA, and CDMA is considerably more complicated and will benefit from performance enhancements techniques that are part of 3GPP Rel. 9 specifications. Hence, Alcatel-

Lucent recommends that Inter-RAT roaming not be mandated for the initial early deployments.

In order to facilitate roaming amongst LTE networks, Alcatel-Lucent recommends that UE interfaces comply with Rel. 8 December 2009 for initial trials and deployments and as a minimum requirement for device backwards compatibility as the network evolves. By requiring common minimum standards compliance for devices, interoperability will be facilitated with multiple vendors' systems. In addition, jurisdictions can leverage the access portal/home page to provide any priority differentiation desired by that jurisdiction.

V. TESTING AND VERIFICATION IS ESSENTIAL IN ORDER TO ENSURE INTEROPERABILITY FOR THE PSBN

Alcatel-Lucent supports the requirement of conformance testing for user devices that will be allowed to operate on the PSBN. This will assure interoperability and avoid harm to the network and other users' data connectivity. In regards to conformance testing for LTE network infrastructure equipment, Alcatel-Lucent employs a rigorous multi-step testing process for our equipment before we consider the equipment to be generally available for purchase by customers. This process involves standalone network element testing for each network element in our solution against the node requirements in a particular release. The lab testing process includes end-to-end feature validation testing and finally network level testing for features that affect multiple functional elements in the network, for example priority access and preemption.

Requirements testing is traceable and documented throughout the cycle. Our products within the solution are then deployed in the field in a First Office Application ("FOA") environment where testing is done in concert with a wireless operator, to

provide objective field testing according to agreed upon requirements. We envision leveraging the National Institute of Standards and Technology ("NIST") Public Safety Communications Research ("PSCR") environment to support FOA testing of Public Safety specific features that are incremental to those tested in normal operator environments. Such a common test environment is critical for public safety networks, since it would not be advisable to introduce new software releases into operational public safety networks serving mission critical applications that have not yet been field hardened in an environment considered typical of public safety networks. We believe that the self-certification process of equipment in light of LTE network and public safety features should meet the needs of the public safety community by allowing for external audit of the company's development and test processes and documented results per TL9000.

Relative to interoperability testing, Alcatel-Lucent recommends that processes in place for interoperability testing on commercial LTE networks should be leveraged. We believe that there are too many interfaces in the LTE network to have vendors affordably validate every possible combination of interface and product/manufacturer/standards release. For instance, in the commercial market interoperability between two vendors on a particular interface is typically achieved in trials and network testing. Detailed results of the IOT testing tend to be proprietary information owned by the two vendors on each side of the interface, with a summary provided to the involved commercial service provider.

We support interoperability testing based on operator request, and recommends that such testing be executed via the well-established process of the Network Vendor Interoperability Testing Forum ("NVIOT") to minimize operator effort and reduce testing

intervals.[4] The NVIOT is an organization of wireless network equipment vendors created to address the industry's challenges of assuring open interfaces and interoperability and reducing the interval required to deploy high-quality multi-vendor networks. The forum accomplishes this by documenting best-practice testing methods, by authoring generic Master Test Catalogs ("MTCs") for network interfaces which are quickly adaptable to specific IOT requests, by providing a template for interoperability testing engagements (from planning through execution, issue resolution, and documentation) that allows re-use of testing results across multiple operator requests, and establishing a basis of agreement between vendors which minimizes effort required by operators to drive vendor coordination. The Forum works in cooperation with standards bodies to address any standards errors or ambiguities found during testing.

Finally, relative to the PSBN, Alcatel-Lucent believes that interoperability across interfaces should be required on those interfaces that will impact roaming and device/application interoperability with the network as outlined in paragraph 110 of the *Fourth Further Notice*. An independent lab facility should be designated, such as the NIST/NTIA PSCR field system, where interoperability testing may be facilitated amongst participating vendors in a neutral environment. In addition, other interfaces should also conform to standards, and may be pairwise tested on an as needed basis with compensation as negotiated amongst specific vendors to respond to a specific market request on a time and materials basis.

[4] The NVIOT Forum was founded in March 2000 by Alcatel, Lucent Technologies, Ericsson, Motorola, Nokia, Nortel Networks and Siemens and has expanded to include most other major infrastructure vendors. The Forum has facilitated interoperability for GSM and WCDMA and its charter was expanded to include the LTE/SAE technologies in May 2008. Specification of MTCs for 3GPP R8 based interfaces, which include those for LTE, started in Q2 2008 and continues to develop Catalogs for LTE interfaces based on operator priorities represented by NVIOT Forum members.

VI. FEDERAL FIRST RESPONDERS SHOULD BE PROVIDED ACCESS TO THE PSBN

Alcatel-Lucent supports the use of the PSBN by federal users. Federal first responders will provide an increase in the demand for devices on the PSBN and will make it more attractive for device equipment vendors to participate in the solution. In regards to control, use, charging model, and capacity usage of the network by Federal users, Alcatel-Lucent's solution is capable of supporting any of the proposed models. In the end, the governance model for the PSBN will lead to an appropriate method for dealing with these issues for Federal users.

VII. SECTION 337 ALLOWS UTILITIES AND OTHER CRITICAL INFRASTRUCTURE ENTITIES TO USE THE 700 MHZ PUBLIC SAFETY BROADBAND SPECTRUM ON A SECONDARY BASIS

The Commission recognizes that enabling utility and critical infrastructure (collectively "CII") access to the 700 MHz public safety broadband spectrum will enhance coordination during emergencies and, importantly, spread the costs for building the public safety broadband network.[5] The *Fourth Further Notice* seeks comment, however, on whether such an approach is consistent with Section 337 of the Act.[6] As discussed below, CII use of public safety spectrum on a secondary basis is permissible under Section 337 of the Communications Act.

When Congress adopted Section 337 and set in motion the DTV Transition across the 700 MHz band (746-806 MHz), it directed the agency to reallocate 24 megahertz of that spectrum "for public safety services according to the terms and conditions

[5] *NPRM* at ¶ 135.

[6] *Id.* at ¶¶ 135-40.

established by the Commission."[7] Section 337, in turn, defined "public safety services" as services:

> (A) the sole or principal purpose of which is to protect the safety of life, health, or property;
> (B) that are provided -
> (i) by State or local government entities; or
> (ii) by nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services; and
> (C) that are not made commercially available to the public by the provider.[8]

The Commission has previously addressed eligibility issues related to the 700 MHz public safety spectrum and Section 337 in the *Second Report and Order* in this proceeding. There, the Commission examined whether a commercial entity – the D Block winner – could access the 700 MHz public safety spectrum for the provision of commercial services.[9] Here, in contrast, the Commission is considering whether the 700 MHz public safety spectrum relevant question relates to use of the spectrum for the provision of CII communications which "support[] public safety entities during the resolution of emergencies"[10] and "play an important role on occasion supporting public safety entities to carry out their mission of protecting the safety of life, health, or property."[11]

---

[7] 47 U.S.C. § 337(a).

[8] 47 U.S.C. § 337(f)(1).

[9] *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150, *Second Report and Order*, 22 FCC Rcd 15289, 15406 (2007).

[10] *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150, *Second Report and Order*, 23 FCC Rcd 14301, 14405 (2008) ("*Third FNPRM*").

[11] *Id.*

In the *Second Report and Order*, the Commission considered Section 337(a)(1) and concluded that it:

> requires neither that the 24 megahertz at issue be allocated exclusively for public safety services nor that it be used only for such services. Moreover, Section 337(a)(1) confers upon the Commission the authority to allocate 24 megahertz for public safety services "according to the terms and conditions established by the Commission." We construe this phrase as affording us broad discretion to impose conditions on the use of this spectrum to effectuate its optimal use by public safety, and the condition at issue here serves just such a purpose.[12]

The Commission recognized that secondary commercial use could harness private sector resources to fund buildout of the interoperable public safety network. Here, CII can play a similar role – with the added benefit that the CII mission significantly advances public safety.

The Commission further concluded that, even if the statute required that the 700 MHz public safety spectrum be used primarily for public safety services, secondary use of the spectrum for non-public safety purposes still would be permitted.[13] Specifically, Section 337(f)(1)(A) defines "public safety services" as those for which "the sole *or principal purpose*... is to protect the safety of life, health, or property."[14] Nothing in the legislative history indicates that Congress intended that the spectrum in question be dedicated exclusively to public safety use. Thus, as the Commission concluded, so long

[12] *Id.* at 15438-39 (emphasis in original).

[13] *Id.* at 15439.

[14] 47 U.S.C. § 337(f)(1)(A) (emphasis added).

as the principal use of the license is to provide public safety services, secondary use of the spectrum for the provision of non-public safety services is permissible.[15]

The *Fourth Further Notice,* however, referenced tentative conclusions proposed in the *Third FNPRM* expressing concern with CII use of the 700 MHz public safety spectrum on a secondary basis.[16] These concerns are unwarranted. First, the *Third FNPRM* appeared to be addressing the issue of primary access to public safety spectrum by CII entities rather than secondary usage at issue here.[17] In addition, the tentative conclusions in *Third FNPRM* were never effectuated and moreover did not address the Commission's prior determination in the *Second Report and Order* that secondary use of public safety spectrum by non-public safety entities is permissible under Section 337.

Similarly, the Commission's decision in the *Public Safety 700 MHz Waiver Order* does not address whether Section 337 permits the secondary usage at issue here. There, the Commission denied Flow Mobile access to the public safety spectrum because it (i) was not a state or local governmental entity, nor was it authorized by such an entity, and (ii) was not seeking access to the spectrum on a secondary basis.[18] It did not address whether secondary usage by non-public safety entities is permissible if such use is authorized by a governmental entity whose primary mission is the provision of public

[15] 22 FCC Rcd at 15439. Certain CII operations are critical to protecting life, health, or property, and the Commission should ensure that any secondary use requirements permit continuity of such operations.

[16] *NPRM* at ¶¶ 134-136.

[17] *See Third FNPRM*, 23 FCC Rcd at 326 ("permitting CII entities to access the 700 MHz public safety spectrum through the Public Safety Broadband Licensee – and thereby access this spectrum on a *priority basis* – would not be in the public interest" (emphasis added)).

[18] *Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks*, PS Docket No. 06-229, *Order*, 25 FCC Rcd 5145, ¶¶ 78-82 (2010).

safety services. Such usage is expressly authorized by the plain language of Section 337,[19] as the Commission properly concluded in the *Second Report and Order*.[20]

In sum, CII communications serve an important public interest objective and support public safety efforts. Given that Section 337 allows for use of the 700 MHz public safety spectrum for services like CII on a secondary basis, the Commission should expressly authorize such use.

VIII. ALCATEL-LUCENT DISAGREES WITH THE COMMISSION'S TENTATIVE CONCLUSION THAT FIXED SERVICES SHOULD OPERATE IN THE 700 MHZ BAND ON AN ANCILLARY BASIS

We respectfully disagree with the Commission's tentative conclusion that fixed services should operate in the 700 MHz band only on an ancillary basis. The Commission should not dictate what applications may or may not be allowed on the 700 MHz PSBN and affix priority on the network, as this potentially could stifle innovation and would not adequately reflect the needs of public safety in a given jurisdiction. In the end, we believe that applications on the network are best left to the network operator, so as to reflect each jurisdiction's operational environment, needs, and risks for use of the 700 MHz PSBN.

[19] 47 U.S.C. § 337(f)(1).

[20] 22 FCC Rcd at 15439.

IX. CONCLUSION

For the foregoing reasons, Alcatel-Lucent urges the Commission to create interoperability requirements that are consistent with the arguments presented herein.

Respectfully submitted,

Alcatel-Lucent

By: _____

Michael McMenamin
Sr. Counsel - Director
Global Spectrum Strategy
LTE Mission Critical Communications

Jeffrey Marks
Sr. Counsel – Director, Regulatory Affairs
Public Affairs, Americas Region

1100 New York, Avenue, N.W.
Suite 640 West Tower
Washington, D.C. 20005

April 11, 2011