

**Before the
Federal Communications Commission
Washington, DC 20554**

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

**THIRD REPORT AND ORDER
AND FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING**

Comments of IPWireless, Inc.

Introduction

IPWireless Inc, ("IPW"), as a major existing supplier of wide-area public safety mobile broadband systems in the USA to both large cities such as New York and smaller cities such as Gillette, is pleased to submit comments on the Third Report and Order and Fourth Notice of Proposed Rulemaking ("FNPRM").

IPWireless is an active contributor to 3GPP standards, and a developer and supplier of end-to-end LTE systems, including Radio Access Network (RAN) infrastructure, Evolved Packet Core (EPC) and User Equipment (UE).

In the response below, IPW provides overall comments on the general philosophy of regulating Mobile Broadband technology to be used by Public Safety, as well as commenting on the specific questions posed by the Commission.

General Comments

IPWireless fully supports the adoption of 3GPP Long Term Evolution (LTE) as the technology for Public Safety Mobile Broadband systems operating in the 700 MHz spectrum allocated to Public Safety. We believe that this standard provides the best possible foundation for the much-needed interoperability between jurisdictions operating such networks, as well as enable Public Safety to take advantage of the multi-billion dollar R&D investment in LTE by the commercial wireless industry, and the economies of scale offered by a mass market wireless technology.

We recognize that the Commission's decision to mandate a specific technology against a long history of technology neutrality was not made lightly, and as noted above IPWireless fully supports this direction. However, we suggest that the scope of technical regulation be limited, to avoid departure from the inherent support for interoperability in the 3GPP standards, and most importantly to avoid inadvertently imposing unnecessary constraints and costs on the public safety community that may impede the rollout of mobile broadband to first responders, and competition in the marketplace. With these concerns in mind, we submit that the regulation should be largely limited to 3GPP standards compliance and the fundamental governance requirements for interoperability.

A basic theme in IPWireless's response to this NPRM is that once standards compliance and fundamental interoperability requirements are met, each jurisdiction should have the freedom and flexibility to decide the deployment that is appropriate for their service area and local operational requirements, have the opportunity to choose from multiple vendors, and especially to have the ability to deploy a network that is affordable to them. For example, while a 256 kbps cell edge uplink rate may be very appropriate for a large city, it may not be required in a sparsely populated rural county, where building the greatest geographic coverage economically may be the primary concern. As an example, IPWireless is currently designing a public safety LTE network for a rural county of some 1600 square miles in which only about 200 mobile users are anticipated to use the network. A design for in-vehicle coverage and a cell edge uplink rate of 128 kbps is the only practical way of making such a deployment economically feasible for the county, absent certain, timely and unlimited Federal funding. There are

other incident level solutions that can be deployed to increase that network capability as needed, and not be required network wide.

Each jurisdiction is, by nature, incented to build a network with reasonable and adequate service levels to meet its needs. Public safety roamers can take comfort in this. Regulating the service requirements of each network, beyond standards compliance and core interoperability requirements, is unlikely to outweigh the benefit of a jurisdiction being able to deploy a network that strikes a balance between their operational needs and available funding. Accordingly, a core premise of IPWireless' argument is that detailed service levels should not be imposed on all networks, and that any roamers (e.g. a Federal agency) which require a higher level of service, should negotiate the terms and share the related increase in costs of procurement on a case-by-case basis.

In many of our comments, IPWireless is proposing what we believe is best for Public Safety rather than what might be best for LTE vendors such as ourselves, as we believe that vendors will ultimately benefit from rules that allow jurisdictions to build networks appropriate to their individual needs and within their financial constraints, rather than rules that result in requirements for excessively large numbers of base stations and support core network infrastructure, as such requirements may be prohibitive for certain jurisdictions from a funding perspective

By adhering to 3GPP standards for e-UTRA (LTE), which is designed to support worldwide roaming and interoperability, agreeing the appropriate architecture within the standards framework, and putting in plan the necessary governance structures, the interoperability requirements of Public Safety should inherently be met. Conversely, requiring interoperability for Public Safety that deviates or goes beyond the 3GPP standards runs a serious risk of losing the benefits (such as economy of scale and user equipment ecosystem) that come from using a mainstream commercial wireless standard, limit number of vendors to the Public Safety community, and worst of all, increase equipment costs. Therefore, any public safety specific requirements that are not supported by current or proposed standards should be proposed to the 3GPP standards body, following their normal processes. IPWireless, as an active participant in 3GPP, is willing to support appropriate proposals for future releases of the LTE standards.

It must be recognized that the 3GPP LTE standards, like GSM and UMTS before it, are designed to support an international "network of networks", with universal roaming of users and interoperability for the full range of services supported. By adopting LTE, requiring the roaming interfaces defined in the standards, and implementing governance structures, the objective of national roaming and interoperability between public safety networks will be achieved.

Beyond the basic requirements of standards compliance and interoperability, many of the questions on technical requirements raised by the Commission in this NPRM are valid and commonsense, however we believe it is appropriate to question whether all of these things should be codified in regulation. As an alternative, IPWireless proposes that many of these could be embodied in a “code of practice” for Public Safety mobile broadband networks. The concept here is that regulations should specify minimum interoperability requirements and 3GPP standards compliance, and the code of practice would provide a guideline for a typical network deployment. The code of practice would be voluntary, but compliance encouraged. Public Safety jurisdictions could chose to either adhere to the code of practice, or deviate from it where they have specific needs or reasons to do so to meet their unique requirements (including budgetary constraints).

Finally, as a supplier of mobile broadband systems to New York City and Gillette Wyoming, IPWireless see the significant of the benefits of “multi-agency” networks, where the network is shared between first-responders and other city / county agencies on a relative-priority basis. The primary benefit of multi-agency networks is through the economies of scale and scope in sharing the cost of a capital-intensive network, but also in increasing the breadth of funding sources, such as Federal and State grants for a variety of services to the public, beyond just Public Safety. We address this in more detail in our response to section F. “Section 337 Eligible Users”.

IV. IV. Fourth Further Notice of Proposed Rulemaking

16. (Interoperability Definition)

This definition is critical, as it is the foundation for interoperability rules, and thus deserves significant attention.

The current definition in Part 90 of Commission’s rules does not make it clear that an entity from any jurisdiction should be able to operate on the network of any jurisdiction anywhere in the nation. The DHS definition, while valid, is heavily focused on voice while the LTE network will provide a range of services including broadband data, voice and messaging.

IPWireless therefore supports the broadening of the definition as proposed by the Commission, with further clarification on what and where users should be able to roam and obtain interoperability. We propose the following revised definition: “Interoperability should allow any authorized user while *in*

their home network or while roaming to be able to access any *Band 14 LTE local*, regional or tribal public safety network in order to reach any other *authorized* users and any *authorized* services at the home network or at visited network”.

IV. A. A. Technical Rules for the Public Safety Broadband Network

1. Architectural Framework

17, 18, 19. IPWireless supports the architectural framework proposed by the commission, with the exception of the following three items which, we believe should be decisions for the individual public safety operator, according to his/her local conditions and requirements: (a) Support of a minimum level of spectrum efficiency, (b) Support of a minimum level of coverage reliability (95%), and (c) support for interference mitigation schemes. To be clear, the LTE technology is capable of supporting these things, but they are very dependent on the radio planning and network design that the jurisdiction chooses, or is force into by funding constraints. We provide detailed comment on these items in the following sections of this response.

We view the architectural framework as a tool in the process of determining the interoperability rules, but the framework itself should not be codified in regulation, for the reasons set forth in this response.

20. Support for Voice and Data Communications:

We support a requirement that the network must be able to support mission-critical voice as well as data. It is imperative that the support of voice is in a manner that is compliant with LTE standards, and that any special public safety requirements are standardized through the 3GPP process, otherwise the benefits of using a large-scale open standard will be lost. Specifically, push-to-talk group calling of the type required by public safety is not currently supported by the 3GPP standards, and the public safety community needs to give urgent attention to developing a statement of service and feature requirements, and initiating a 3GPP Study Item for this issue.

21. Roaming Authentication and Internetworking Functions – Clearing House

IPWireless supports in principle the use of a common clearing house for inter-network roaming, as this is the standard approach used to roaming between commercial 3GPP networks. Such a clearing house

could either be established specifically for public safety, or through the selection of an existing commercial clearing house. Should an existing commercial clearing house be used for this purpose, then the Commission or an appropriate public safety body will need to ensure that reliability and disaster resilience requirements of public safety are met, otherwise the clearing house will become the weakest link in interoperability, and to ensure competition in the provision of clearing house services

22. Nationwide Backbone Network

IPWireless' comments on this subject are provide in our response to Section 8

23. Nationwide Services and Capabilities

We support the concept of a nationwide public safety LTE network achieved through a network of networks, using the same 3GPP roaming and interoperability mechanisms as used by commercial operators to achieve a similar, but worldwide, network. We caution against any concept of a single core network and/or backbone network for public safety, as this could create a single point of failure, increase backhaul transmission costs, risk failure in a major disaster when it is needed most, and potentially impede the prompt rollout of networks. Local or regional networks should have the option of forming mutual backup arrangements between themselves, for example where one jurisdiction's EPC and / or HSS/PCRF provides backup for a neighboring network and vice-versa.

24. Evolution

Please refer to IPWireless' response in "Technology Platform and System Interfaces (29)" below

26. Evolution of Architectural Framework

We believe that it is appropriate for the Commission, perhaps through ERIC, to evolve the architectural framework over time to reflect evolution in standards and technology, however as noted in our comments above on "Architectural Framework", this framework should not be codified in regulation. The LTE technology companies, PSCR and public safety operators and organizations represented on the Public Safety Advisory Committee are best equipped to provide the Commission with advice on technical advances that may need to be taken account of in a review process.

3. Open Standards

27. The adoption of the 3GPP LTE standard for public safety mobile broadband networks is the ideal way of ensuring open standards, as the 3GPP standards are both open and international.

28. On the question of use of “patented technologies”, it should be recognized that many companies have patents and IPR covering LTE in 3GPP Release 8 and beyond, however there is already a 3GPP IPR policy and working arrangements within the vendor community to deal with this, which has proven very effective in commercial adoption and widespread use of 3GPP standards (which would not have occurred with restrictive IPR practices). The real danger would be if the Commission (perhaps inadvertently) required the use of patented technologies that are not within the 3GPP LTE standards for the UE RAN and EPC elements, and the widely adopted IETF standards for the Internet aspects of the network, as this would undermine the benefits of using a single open standard.

Consistent with IPWireless’ view on the critical importance of adherence to 3GPP LTE standards, we generally oppose any proposals to require proprietary requirements on top of the 3GPP standards. Instead, where public safety requires a service or feature that is not supported in the current standards, these should be standardized through the 3GPP process, otherwise the interoperability and ecosystem benefits which lead to the decision to adopt LTE will slip away. As stated in “Technology Platform and System Interfaces” and “Support for Voice and Data Communications”, voice and messaging services over the LTE network should rely on the 3GPP standards, and new services such as group call voice public safety communications should be standardized in 3GPP.

4. Technology Platform and System Interfaces

29. 3GPP standards are already agreed for Release 9 LTE, and in development for Release 10 and beyond. It would be inappropriate to require that public safety LTE networks be upgraded to support all the requirements of future releases at specific dates, as some of these may not be applicable to public safety and may unnecessarily increase costs (such as requiring unnecessary replacement of user equipment), as well as creating revenue recognition problems for those vendors which are public companies. It should also be noted that not all features in 3GPP standards are mandatory. Individual jurisdictions should have the flexibility to implement upgrades on their own timeframe based on performance needs and as resources/funds permit. Because a fundamental feature of 3GPP standards

is support of backward compatibility, Release 8 LTE will be the standards basis for interoperability, allowing roaming to and from Release 8 and upgraded networks. IPWireless therefore proposes that 3GPP Release 8 be defined as the baseline, and that adoption of future releases should be optional, with the exception of feature such as standardized push-to-talk group voice calls, and relevant multicast and broadcast standards, support of which may be mandated by the Commission once relevant 3GPP standards are published, and where there is a clear need for public safety interoperability. Similar requirements that arise in the future should be treated on a case by case basis, and mandated by the Commission only where there is a compelling need, as agreed by the public safety community.

The requirements for interoperability between networks are well covered in 3GPP release 8. As a general statement, the new requirements in Releases 9 and 10 are enhancements to performance and new features that have minimal impact on interoperability, with the exception of items such as push-to-talk voice over LTE and short messaging , which are not yet fully standardized. As 3GPP standards support backward compatibility, it is feasible for different networks to operate on different releases. It is only future standards such as for group call voice that may need to be mandated in future, but this does not required mandating of the entire 3GPP Release containing such features.

Voice over LTE (using an IP Multimedia Subsystem or “IMS”) is standardized in 3GPP, but it is widely recognized that “profiles” or subsets of the broad specifications needs to be agreed so that a common ecosystem of UEs and infrastructure can develop. Push to talk group call voice over LTE is yet to be standardized, as discussed above. Because of the importance of voice in public safety applications, it is logical for compliance with future 3GPP standards for voice to be mandated for public safety networks. However, while we are advocating that compliance with 3GPP standards for voice be mandated, we do not believe that it is appropriate for implementation of voice on public safety LTE networks to be required by the Commission by any particular date, as some jurisdictions have or will have P25 mission critical voice networks that fully meet their voice needs for a long time, and therefore the cost of implementing voice over LTE may be unwarranted (and potentially unaffordable).

In respect of video, future standards will support video through IMS based enhanced multimedia services such as bi-directional unicast video and through eMBMS broadcast standards (downlink). eMBMS broadcast video is expected to be important for providing incident and other video to large groups of first responders while minimizing the impact of video on network capacity. In line with our recommendations above on voice over LTE, we propose that that any IMS or eMBMS video services implemented should be required to be compliant with existing and future 3GPP standards, and that the

decision to implement video services within any network be at the option of each jurisdiction according to their own requirements.

30. (IPv4 and IPv6):

The IPWireless LTE network and devices will support both IPv4 and IPv6, as we expect that commercial networks will use a mix of both over time. We note that the relatively small number of users (<1 million) in public safety should not create any unusual pressure on IP address resource, but if the scope of usage of band 14 networks is extended to utilities, machine-to-machine communications could increase the number of addresses required significantly. The greatest issue is therefore likely to be the support of IPv6 by equipment such as servers and remote computing devices beyond the scope of the LTE network itself.

31. (Tunneling Protocol in LTE)

We believe that most if not all implementations of LTE for commercial operators use the GTP tunneling protocol, and therefore it is logical for public safety networks required to use GTP for the purposes of interoperability, as well as to gain the benefits of using the same standard as commercial networks. It is our understanding that the PMIP option in the 3GPP standards exists primarily to allow integration of LTE with non-3GPP networks which is unlikely to be a significant requirement of public safety networks. External PMIP implementations for session continuity over LTE and other non-3GPP networks can still be implemented if required.

5. System Identifiers

The Commission's consideration of methods to minimize the number of system identifiers required by public safety is based on the assumption in the NPSTC BBTF Report, that only one-hundred or fewer network identification numbers may be assigned. IPWireless questions this assumption on the following grounds:

- The US is allocated seven Mobile Country Codes (MCC) - 310 through 316 inclusive
- Each MCC can support 999 mobile network codes (MNC). Per 3GPP 36.331 and 23.003, the MNC can be 2 or 3 digits, but this is set up in the E-UTRAN, and as we would expect most networks to be able to support a 3 digit identifier, this should be made a requirement.

- A total of 6993 networks can therefore be supported in the US
- The commercial networks are using a total of 210 MNCs¹. With the exception of 2 networks in MCC 316, all of these are in MCCs 310 and 311
- 6783 MNC's are therefore available, and those in MCC 312, 313 and 314 are totally unused

The allocation of MNC's is managed by Telcordia, and while it is reasonable to expect them to conserve MCC/MNC resource, this is not an issue based on the numbers shown above, and should not be done at the expense of creating unnecessary constraints on the public safety community, or forcing public safety to use sub-optimal network architectures.

While the number of PLMN ID's should not be a limiting factor based on the above, we recognize that there may be many practical reasons why, at the extreme, not every city and county should need to have a separate PLMN ID. Practical considerations include:

- The size of the UE PLMN ID list for roaming network preference. However, that this is of primary concern for commercial networks where there may be more than one operator in an area. In the case of public safety a roaming UE would normally only see one network.
- Clearing house capabilities and costs to manage roaming transactions for a large number of PLMN IDs
- The number of IPX links required to a clearing house

Taking these considerations into account, IPWireless believes that there will be a natural incentive for each smaller jurisdiction operating a network to work with others on a regional basis for a shared PLMN ID and where necessary, and shared HSS (but ensuring that the HSS or the links to the HSS do not become the point for example in a major natural disaster). Such a region might be a conurbation such as the San Francisco Bay Area, a state (especially for the smaller states in terms of population), or a FEMA region (10 in total). Therefore, in practical terms, there may be less than 100 – 200 PLMN IDs required. Because these regional groupings would be based on unique considerations within each region, we believe that they should be determined locally rather than centrally regulated.

¹ see <http://www.imsiadmin.com/ByHNIns.cfm>

In the above scenario of regional groupings under common PLMN ID's where the number of HSS's will be reduced, a clearing house arrangement should be satisfactory for achieving roaming and interoperability. The benefit of this approach is that is the standard and time-proven method for roaming between 3GPP networks.

An alternative suggested by Alcatel-Lucent and Motorola in responding to the Technical Public Notice, and also supported by the District of Columbia and PSCR, is a hybrid scheme in which one separate PLMN ID would be assigned to each regional or tribal network and a single PLMN ID would be assigned for the overall nationwide network. We note that this does not necessarily conserve system identifiers, but is an alternative to implementing or using a roaming clearing house. We view this as being worthy of consideration, but there are several issues with this approach that need to be taken into account:

- The support of dual PLMN ID's on the eNodeB is defined in the standards, as it is used for RAN sharing between commercial operators. We expect it to be supported by most vendors, but would need to be mandated by the Commission.
- The UE will need to support a multiple PLMN ID list (which would give priority to connection to its home network). This is not mandatory in the standards.
- A roaming UE would normally use the national PDN-GW, and its traffic would effectively be "local breakout" to this gateway. In this architecture, a roaming UE can still potentially use "local PDN-GW breakout" in the regional network, despite the fact that it is using some components of the national EPC, allowing traffic to be routed to the local jurisdiction for participation in mutual aid applications etc.
- Mechanisms and governance will be needed to manage relative QOS / priority on each eNodeB, to prevent roaming users from taking excessive capacity, and the converse.

6. Roaming Configurations

35. IPwireless supports the Commission's proposal to require networks to support both local breakout and home routed configurations, as it is logical that both of these will be needed to support roamers and their applications requirements effectively.

36. In the case of roaming to commercial networks, commercial operators should be encouraged to accommodate public safety roamers, but we support voluntary arrangements. However, we do believe it would be beneficial for some user equipment to support all 700 MHz band classes, as well as other LTE band classes at other frequencies, but this should be optional for each jurisdiction, based on the local, regional and national carriers servicing their immediate and adjacent operational areas

7. Roaming Authentication and Internetworking Functions

37. As per our comments in “Roaming Authentication and Internetworking Functions – Clearing House” above, IPWireless agrees that a common clearing house(s) for public safety is logical. We are however concerned about the potential to lose links to a clearing house (which may be out of state) in the event of a regional disaster affecting transmission routes. We therefore suggest that consideration be given to architectures that also support direct authentication links between adjacent or regional networks likely to be involved in mutual aid, in addition to links to a common clearing house(s).

8. Interconnectivity of Regional or Tribal Broadband Networks

The use of the IP protocol to carry the external system interfaces of an LTE / EPC network provides inherent flexibility to support routing of interconnect traffic over multiple interconnect routes, as may be required for capacity, performance, redundancy and diversity reasons. Coupled with this capability, we believe it is logical that both direct interconnection between jurisdictions and centralized interconnect will be necessary, and therefore should be permitted.

Local or regional networks minimize the bandwidth requirement for interconnect between networks, as the nature of public safety mobile broadband is that most traffic is between local users, or between local users and local servers. Roaming traffic is expected to be relatively small in proportion as mutual aid by definition is engaged primarily in local communication. In the case of Federal users for example, if they have significant traffic to remote servers, they should be expected to provide or bear the cost of the required transmission facilities or capacity.

Locating EPC elements within the local or regional networks also allows long distance capacity requirements to be minimized.

The public Internet can serve effectively as a common, universal interconnect cloud for regional networks, as it inherently provides redundancy and diversity through its dynamic routing capabilities and underlying support of multiple routes through multiple carriers. This can be supplemented by direct interconnect transmission between adjacent or nearby jurisdictions with a significant requirement for mutual aid, using dedicated links or managed services from carriers.

Direct interconnection between adjacent jurisdictions with significant cooperation requirements is likely to be necessary to ensure effective roaming interconnect for mutual aid responders, as there is a risk that long distance transmission links to a centralized interconnect facility could be lost, for example in a major earthquake or act of terrorism or war. The Commission's Notice of Inquiry (NOI) "FCC Explores Ways to Further Strengthen the Reliability of America's Communication Networks" released on April 8 2011 is very timely and pertinent. It would be ironic for the outcome of this FNPRM to recommend centralized architectures for public safety that contradict the move to strengthen reliability in a major disaster.

There are also expected to be situations where adjacent jurisdictions agree on mutual EPC backup, where the EPC in one network provides geographically redundant backup to the network of an adjacent city or county.

On the question of a common clearing house for roaming, please refer to IPWireless' comments above under "Roaming Authentication and Internetworking Functions – Clearing House".

9. Prioritization and Quality of Service

As the Commission has identified, the LTE standards provide a powerful set of capabilities for both user and application prioritization, which are supported in IPWireless LTE products, along with other vendors' products.

It is important to recognize that the LTE standards provide a "toolbox" of capabilities for QOS / prioritization, and the way in which they are configured and the way in which policies are implemented, determine the actual prioritization service. In combination with appropriate policies, we believe the toolbox provided by the standards (in ARP and QCI and in access class control) will be totally adequate.

We do not believe there will be a “one size fits all” prioritization plan that suits all public safety jurisdictions, as all have varying requirements. Accordingly, we suggest that the implementation of a particular priority scheme should be the responsibility of the individual jurisdiction or regional network operator, but it may be appropriate for an agreed voluntary “code of practice” to be developed by the public safety community, which is essentially a governance requirement.

In the case of prioritization for roamers, there is an obvious role for such a code of practice, to ensure that inbound roamers do not use an unduly high level of priority. However, jurisdictions will need the flexibility to negotiate variances from this to deal with local requirements.

10. Mobility and Handover

The Commission is correct that the LTE standards support handover between cells for continuity of service (“seamless coverage”), and also as a key factor in managing inter-cell interference in a network (handover prevents a user from “stretching” a cell into the area normally covered by another cell and causing unnecessary interference). This is a fundamental feature of the LTE standard and networks will not perform effectively without it. Because it is inherent in the LTE standard, which the Commission is requiring, there is no need to mandate or regulate the implementation of handover.

During active sessions, the choice of X2 or S1 based handover will not impact overall interoperability between operators, and therefore does not need to be regulated by the Commission. The decision to handover is controlled in both cases by the serving eNodeB. Both procedures provide an optimized handover with either direct tunneling in the case of X2-based or indirect tunneling in the case of S1-based handover. The key difference is that support of X2-based handover requires X2 connectivity between eNodeBs involved in the handover. This may or may not be practical within an operator’s particular network, and because it does not impact interoperability, it should therefore be left to individual jurisdictions to decide.

The LTE standards allow roaming and handover between networks of different operators, i.e. across a geographic boundary where coverage from the two networks overlaps. Roaming and handover are different things: whether or not handover is implemented between adjacent networks does not affect roaming, and should be the decision of the local jurisdictions based on their operational needs. For example, jurisdictions should not be forced to build overlapping coverage to support handover if they do

not need it. In order to facilitate handover in to adjacent networks, operators will need to coordinate network planning between themselves. Prior to a handover between different networks, the eNodeB currently serving the UE contains UE context information including roaming restrictions. A key parameter of this information that controls handover between neighboring networks is the Handover Restriction List. This list includes entries for allowed PLMN, restricted Tracking Area (TA), and restricted Location Area (LA) for the UE during handover. As such, prior to initiating a handover, the serving eNodeB will check if the UE is allowed to handover to the PLMN and TA/LA associated with the target eNodeB. During handover, assuming separate EPC between jurisdictions, both S-GW and MME will be changed. However, the PDN-GW will remain the same as prior to handover. Since the PDN-GW provides the IP anchor point, no session discontinuity is experienced. There is no provision in the standards for local breakout in a handover situation between networks.

Regardless whether handover is within or between networks, it is essential that proper RF planning be performed such that sufficient levels of cell overlap exist to enable handover to occur before connectivity to the serving site is lost. In the case of handover between neighboring jurisdictions, this will require optional coordination, as discussed in “Interference Coordination (76-79)”.

LTE supports vehicular mobility at speeds up to 350 km/hr (217 MPH), and therefore we do not see any need for to the Commission to regulate a minimum performance level. Likewise, a UE roaming onto another network can perform this at similar high speed, as roaming authentication on another network is not speed-dependent in itself.

11. Out-of-Band Emissions and Related Requirements

IPWireless generally supports the use of common transmitter emission masks across multiple bands and markets, which is especially important to the goal of public safety being able to take advantage of the commercial ecosystem of LTE. In the case of the US, we support the Commission’s “43 + 10logP” mask, which applies to most commercial cellular bands.

In terms of coexistence between the public safety broadband allocation and the D block, it must be understood that adjacent channel interference is probabilistic, and even with more stringent transmitter emission masks and enhancement blocking and adjacent channel selectivity in receivers, interference will cause problems in a small percentage of situations. One way that the major commercial mobile

operators avoid this by redirecting a victim UE to another of the operator's bands, on the basis that coexistence "outage" areas will not normally correlate between bands.

In analyzing adjacent channel coexistence, there are several scenarios that can cause interference, including:

- Adjacent channel base station to public safety UE
- Adjacent channel UE to public safety base station
- Public Safety UE to adjacent channel base station
- Public Safety base station to adjacent channel UE.

While IPWireless does not advocate any change to the commission's rules on out-of-band emissions for the public safety broadband block in this case, if changes are required we would suggest that they be restricted to base station transmitter emissions and receiver performance requirements, on the basis that the changes to UE requirements would impact the ability to take advantage of the commercial UE ecosystem and may result in higher costs. Though outside the scope of this proceeding, it should be noted that prior to allocation of the D-block, out-of-band emissions from the D-block into the public safety broadband block need to be defined.

The primary coexistence concern is between the public safety broadband spectrum and the D Block. Coexistence issues as described above could be mitigated either by collocation of public safety and D block base stations, allocating to the D Block to Public Safety to use as a 10 + 10 MHz LTE system. However with the D block allocated to public safety, the coexistence issue would simply shift to the C block, even with the 1 MHz guard band that exists (this guard band has only minimal benefit to coexistence).

12. Applications

In the context of ensuring interoperability, we suggest that the Commission's role should be to regulate the *network access* to public safety applications, but not to regulate the applications themselves, as this is logically a function of existing public safety organizations. We do note that the five "applications" listed in by the Commission, with the possible exception of "status information or home page", in this proceeding are in reality requirements to provide access, or "connectivity requirements" rather than the "applications" in the true sense.

A standards-compliant LTE network is designed to carry Internet Protocol (IP) traffic, and is transparent to protocols within “IP”, such as HTTP, HTTPS, FTP, L2TP etc. Therefore, by requiring compliance with 3GPP release 8 LTE, the goal of providing unrestricted and interoperable access to public safety applications should be met without the need for further regulation.

Likewise, a LTE network is also transparent to VPN protocols such as IPSec, PPPTP and L2TP. The question of “what VPN protocols should be allowed” is therefore not a network one, but one that is interrelated with the question of standardization of public safety applications access. Even though LTE networks can be interoperable with each other, access to public safety *applications* will not be interoperable unless there is standardization of VPN protocols used, and agreed user authentication policies / governance. IPWireless therefore recommends that a VPN protocol be agreed upon by public safety, and that a common VPN user authorization scheme be considered, alongside the related authentication issues of HSS interoperability and PLMN ID’s.

The Commission has listed for “desired” applications, which we address below:

Location Based Data Capability: This needs to be better defined, however LTE network can support GPS and other location techniques, and applications that make use of location information.

One-to-Many Communications Across all Media: As per IPWireless comments in other sections of this response, we believe that voice group calling and video / data multicasting and broadcasting will be required, and these require further development within the 3GPP standards. As these features require specific support in the standards, they should be viewed as services rather than applications.

LMR Voice: See IPWireless comments in “Technology Platform and System Interfaces” and “Support for Voice and Data Communications”.

PSTN Voice: As noted elsewhere in this response, PSTN voice will be supported by LTE networks in the future by Voice-Over-LTE, using IMS.

57. Real time voice and video:

Real time voice is a service that will be supported by LTE networks in the future, but as noted in our response to “Support for Voice and Data Communications (20)” above, standards work in 3GPP for push-

to-talk group call voice needs to be initiated by the public safety community. In this way, 3GPP standardization will ensure interoperability for real time voice, without losing the ecosystem benefits of adherence to 3GPP standards.

Both voice and video (2 way unicast) in LTE will be supported by a standardized IP Multimedia Subsystem (IMS). Consequently, interoperability for both voice and video is addressed by the LTE standards, and should not need to be regulated separately.

SMS messaging over LTE is supported in the current release, however for non-legacy operators, it is reliant on IMS profiles being agreed, and IMS systems becoming available, While other IP-based messaging applications can be used as an interim, we suggest that public safety adopt the LTE standard SMS service for interoperability, in order to ensure compatibility across the full range of LTE UE's, and to take advantage of the commercial ecosystem.

13. Interconnection with Legacy Public Safety Networks

Interconnection of public safety LTE networks with existing narrowband networks such as P25 is expected to be a requirement for many jurisdictions in the future, as they transition from legacy networks to the LTE network for mission-critical voice and related applications. However, interworking of the two networks may not be required by all jurisdictions, and therefore should not be a regulated requirement, as doing so would impose unnecessary costs on some agencies.

Furthermore, "interoperability" between these networks needs to be defined, for example is it limited to bridging of calls between networks, or does it also require dual-mode user devices / radios that support both LTE voice and legacy voice standards?

We note that support of push-to-talk group call voice support on LTE is going to be required for effective interworking with legacy public safety networks. As discussed in "Support for Voice and Data Communications (20)", this requires standardization work in 3GPP, which is yet to be initiated.

While gateways are a current solution for basic interconnection to P25 and other public safety narrowband networks using VoIP, it should not be presupposed that separate gateways are the only solution: it is possible that future equipment could integrate such functions.

14. Performance

As an LTE vendor, IPWireless might be expected to encourage requirements that increase the amount of equipment required in networks, however we believe that giving individual jurisdictions the flexibility to deploy networks that meet individual requirements and budget constraints will result in a better outcome in the long run, which will ultimately benefit public safety and the communities they serve.

As noted in IPWireless' "General Comments", we believe that once standards compliance and fundamental interoperability requirements are met, each jurisdiction should have the freedom to decide on the network performance that is appropriate for its service area and operational requirements, have the opportunity to choose from multiple vendors, and have the flexibility to deploy a network that is affordable to them.

While LTE networks are often designed for cell edge uplink data rates of 128, 256 or 512 kbps (the uplink being the limiting link), these figures are somewhat arbitrary. The cell edge rate that is required in any jurisdiction depends on their operational requirements and applications, and on their user population.

Every doubling of the cell edge uplink data rate (e.g. from 256 kbps to 512kbps) results in an approximate 3dB reduction in link budget, and an increase in the required number of cells and therefore the capital cost by over 30%. Beyond 3 dB, the number of cells required goes up exponentially with every 3dB increase: a network supporting 512kbps cell edge uplink compared to 128 kbps will cost more than double. If deep indoor penetration margins are added to this (as an example), the cost of a network can be multiplied several times.

Accordingly, IPWireless respectfully suggests that the Commission should generally limit its regulation to interoperability, and not attempt to regulate performance. Any remaining concerns about network performance could potentially be managed by Government funding agencies in the future, imposing minimum performance requirements as a condition of funding, or tiered funding schemes tied to performance requirements. In terms of performance in relation to interoperability, we suggest that whatever level of service a jurisdiction decides is appropriate to its needs, should by definition be acceptable to public safety roamers into its territory, and if such roamers (e.g. a Federal agency) require a higher level of service, then it should negotiate a sharing of the costs of providing this. (Please refer also to IPWireless' comments in the Introduction.)

15. Network Capacity

As the Commission has stated in 63; “as commercial technologies become increasingly efficient, it is important to ensure that public safety broadband networks are able to capture these efficiency gains”. IPWireless agrees, and given that LTE is the most spectrally efficient mobile broadband standard, the choice of LTE for public safety 700 MHz networks inherently goes a long way to meeting this goal. In addition to the techniques used in the LTE technology to maximize spectral efficiency, the other key factor is the quality of the radio planning of the network, where there is a natural incentive for jurisdictions to design the best quality network, within the constraints of their actual needs, available tower assets and funding.

For example, a rural jurisdiction with a small user population may chose to deploy using their existing “high site” tower assets, which can increase overlap and interference between cells, reducing spectral efficiency below the theoretical maximum, but fully meeting their capacity needs. In terms of “spectral efficiency” in situations like this, we suggest that the focus be on *efficiency of the network in providing the capacity to meet the needs of the jurisdiction*, rather than the theoretical maximum spectral efficiency of a (dense) network built where cost is not taken into account.

The Evolved Packet Core (EPC) supporting an LTE network is typically easily and economically scaled to handle the full throughput of a population of eNodeB’s, so this should not be an issue of concern to the Commission.

In terms of backhaul, the transmission serving each cell site can be sized according to the actual traffic from users, rather than the theoretical peak capacity of the eNodeB’s supported. Support of peak sector capacity may be desirable in areas with large numbers of users, to support a situation where an incident occurs close to the cell site, where most users are on high modulation and coding steps, however as the backhaul serves all 3 sectors on statistically multiplexed basis, it would be less likely for such a user concentration to be active on all sectors at the same instant in time. As backhaul transmission can be an expensive and significant component of the network cost, it would be unreasonable to require jurisdictions to deploy backhaul capacity that is beyond their needs and potentially beyond their budget. In consideration of these points, the backhaul capacity should be determined by the individual jurisdiction based on their need and financial constraints. In terms of whether “interoperability be impaired if we leave capacity considerations to localities”, IPWireless’ comments in the “Performance” section apply.

As per IPWireless's comments in Section F. "Section 337 Eligible Users", expanding the definition of eligible users to include other government agencies and utilities will increase the efficient use of network capacity, with these lower-priority applications making use of network capacity when it is not being fully utilized by first responders.

16. Security and Encryption

We support the requirement that both mandatory and optional network access security features be required for public safety LTE networks. In particular, public safety networks should be required to implement:

- Cipherring of User plane traffic (using either SNOW 3G or AES based algorithm)
- Cipherring of RRC & NAS signaling (using either SNOW 3G or AES based algorithm)
- Cipherring of S1-U and X2-U traffic (per NDS specification)
- Cipherring of S1-MME and X2-C (per NDS specification)

While these features cover user plane traffic between the UE and EPC, it is vitally important that all links between user client and an application server be secured. We suggest that all public safety entities employ end-to-end security via the use of VPN, which is beyond the scope of 3GPP standards, although LTE networks should carry VPN traffic transparently. (See IPWireless comments under "Applications" above). With respect to network domain security, we recommend that public safety implement both the mandatory and optional features to secure control plane signaling between EUTRAN and EPC elements. In addition to securing intra-domain signaling, the requirements set forth in TS 33.210 provide a basis for interworking and roaming agreements between public safety entities. To fully secure the EUTRAN and EPC, we additionally recommend that both EUTRAN and EPC elements be physically protected.

The application domain security specifications detailed in the referenced documents (TS 33.102 and TS 31.111) cover the secure communication with application resident on the USIM. As stated above, end-to-end security is vital for secure communications. However, beyond the scope of native IMS supported applications such as voice and messaging, the degree and type of security built into applications should be the role of the public safety entities, but noting that in the case of applications shared with roamers there must be an agreed access security (user login etc) approach, in line with IPWireless' recommendations above on VPN user authorization.

With regards to visibility and configurability, these features were intended to ensure security in uncontrolled roaming scenario, such as international roaming, since while the standard highly recommends ciphering, it is an optional feature. In contrast, per the support above, all public safety LTE networks should implement the optional security features. As such, concern for security when roaming to a non-secure network is negated, as by definition public safety will be roaming to other public safety networks with common security measures. Additionally, the details of the ciphering indicator (required for security visibility) is implementation specific and very much dependent on nature of each UE. While some UEs will be equipped with displays that are capable of showing a ciphering indicator, others such as USB Modems will not have displays. It is also important that the level of security required for a specific application not be reliant on active user checks, but rather based on required implementation of all security features. We therefore reiterate our support for implementation of the optional security features and believe this negates the need for visibility and configurability of security.

17. Robustness and Hardening

In IPWireless' view, this is an area where the local jurisdiction should decide what level of robustness and hardening is appropriate to their operational requirements, specific risks in their area and available budget.

18. Coverage Requirements

Coverage requirements will differ widely across the country, according to geography, population distribution, and varying operational needs. An example would be a mountainous area that is expensive to cover, while having a small user base and minimal operational needs. It would therefore be arbitrary for the Commission to define a one-size-fits all coverage requirement.

In line with our other similar comments throughout this response, IPWireless does not view coverage requirements as being within the reasonable scope of interoperability rules: by definition the coverage that a jurisdiction decides is appropriate for its needs and financial constraints should also be appropriate to roaming users into that area. If inbound roamers (e.g. Federal agencies) require a different level of coverage, then they should negotiate that on a case-by-case basis and contribute to the cost of provision. This is not to say that coverage requirements could not be a condition of Federal funding, as there would then be a direct link between the extent of coverage and the funding required to build it.

19. Coverage Reliability

Coverage can be viewed in two dimensions – geographic extent of coverage, and “depth” of coverage. The depth of coverage includes building penetration margins, vehicle penetration margins (for portable devices inside vehicles) and UE antenna gain. All of these can differ widely, making it inappropriate to define standards on a national basis.

As noted in other IPWireless comments, as the requirement for the depth of coverage increases, the cost of a network increases exponentially. As we note in the “In Building Coverage” section below, a network built for handheld UE coverage with a 12 dB building penetration margin would cost approximately 10 times more than a network built for outdoor coverage to vehicle terminals.

Consistent with IPWireless’ comments above on “Coverage Requirements”, we suggest that the individual jurisdiction is best placed to decide on the coverage reliability or depth of coverage required, as well as the coverage they can afford.

20. Interference Coordination

By mandating a single technology to be used in the public safety spectrum, the Commission has gone a long way towards ensuring interference free operation in the public safety broadband allocation. LTE was intended from the outset to operate as single frequency network technology (N=1 frequency reuse). In examining interference coordination further, we view this subject consisting of (a) border coordination, (b) internal interference mitigation within an operator’s network, and (c) adjacent channel interference / coexistence. IPWireless addresses each of these in the following paragraphs. With regards to interference management in general, because interference management relates to performance, and as suggested above in the “Performance (59-62)” section, performance requirements will vary from entity to entity, interference mitigation techniques fall outside the requirements for interoperability. As such, they should not be mandated by the Commission.

In terms of border coordination, clearly borders first need to be defined, either by the Commission, the PSST or by delegated regional organizations. Assuming this is done, we agree that it is appropriate for public safety network operators to notify adjacent jurisdictions of their deployment plans and planned coverage near borders, as is the de-facto practice with many commercial operators. Given the single

frequency reuse of LTE, neighboring networks can operate with minimal levels of coordination, no different in principal to managing interference within an operator's own network. With regards to coordination efforts, one option would be to regulate a signal level at borders, using a definition such as power flux density. However, the levels that are practical would differ depending on whether the boundary is in an urban, suburban or rural area, and whether or not handover is required between adjacent networks (note to be confused with roaming) Please refer to our comments in 10 "Mobility and Handover". Therefore, the most practical would be for adjacent jurisdictions to be required to coordinate border signal levels between themselves. An LTE network sees interference from an adjacent network the same as from other cells in the same network, so a general guideline would be to coordinate a similar amount of cell overlap across borders as between cells in an operator's own network. This level should be based on agreement between jurisdictions and represent their agreed upon extent and depth of coverage, and whether or not handover between networks is required. To achieve this requires a coordinated effort to effectively RF plan along the border. While such activities are recommended, as with intra-network RF planning, IPWireless believes that the degree of optimization and coordination should be left to the individual jurisdictions involved. Nevertheless, we agree that coordination agreements between neighboring jurisdictions are required to protect both parties.

In terms of internal interference mitigation, IPWireless believes that the Commission should not mandate a specific technique. As with previous 3GPP releases, the current LTE and EPC standards detail items that are required to enable a multivendor ecosystem and interoperable communications. The LTE standard does not specify the techniques and algorithms to be used for air interface scheduler or receiver implementation, which are the areas where interference mitigation can be implemented. This approach enables industry wide innovation and associated performance gains within the standard without sacrificing interoperability. In the same vein, beyond ensuring interoperability, the Commission should not, in this context, limit operators to specific interference mitigation techniques, because in the long run this will stifle innovation and potentially lead to unique products being required for public safety, jeopardizing the benefits of the LTE ecosystem.

The Commission asks if static Inter-cell Interference Coordination (ICIC), or semi-static Inter-cell Interference Coordination (ICIC) should be required. In examining ICIC specifically through simulations, IPWireless observes that requiring its implementation would hinder rather than improve network performance:

There is currently only limited support for ICIC in the Release 8 standards, in terms of basic signaling on the X2 interface between eNodeB's, which allows only static ICIC or semi-static ICIC to be implemented. Interference indication messages between adjacent eNodeB's via the inter-eNodeB X2 interface allows semi-static ICIC with limited coordination. With semi-static ICIC, measures to avoid interference are only invoked when interference is detected, for example when scheduling resources to users in the cell edge overlap. This results in more efficient operation than Static ICIC, but is slow to respond to interference conditions (on the order of seconds) resulting in reduced throughput.

Hybrid ARQ (HARQ) is fundamental to intercell interference mitigation in LTE. Through a series of simulations, IPWireless concludes that uncoordinated full bandwidth scheduling ($N=1$) with proper application of HARQ as supported in the standards provides the optimal approach for handling intercell interference over a variety of ICIC schemes including Fractional Frequency Reuse (FFR), Soft Frequency Reuse (SFR), and Voidance Fractional Frequency Reuse (vFFR). Though results vary between technique and associated parameters, reduction in cell capacity resulting from these schemes could be as high as 33%. For all ICIC schemes, the impact is due to two effects: resource limitations imposed by the ICIC schemes, and reduced ability to take advantage of the multiuser diversity in the frequency selective channels with a frequency dependent scheduler. There are a number of other interference mitigation techniques that can be applied in LTE, many of which can be vendor-specific but do not affect standards compliance. In many cases, the choice of interference mitigation techniques depends on the deployment, for example issues are very different in urban versus rural deployments.

IPWireless has long been a leader in interference mitigation on 3GPP technologies. For example, our "GMUD" intercell interference cancellation technology on 3GPP Release 7 TD-CDMA (as used in the New York City "NYCWIn" network) is the most advanced in the industry. In LTE, IPWireless implements a combination of interference mitigation techniques, and will continue to enhance these as we research and develop new technologies, and as 3GPP standards support evolves with each release.

While IPWireless does not support mandating network performance, requiring specific ICIC implementations could significantly increase the cost of implementing a network, through reducing capacity per cell. As shown above, striving to minimize the impact of interference at the cell edge, can lead to a 33% reduction in sector capacity. If the network must meet a specified spectral efficiency over

a geographic area, then with ICIC, 33% more sites would be required to deliver a certain network capacity, thereby increasing the cost of a deployment by one-third.

In terms of adjacent channel interference / coexistence, as discussed in section “Out-of-Band Emissions” (51-54), IPWireless agrees with the Commission’s proposed revisions to the OOB rules. Furthermore, the decision on the D-block allocation will largely drive whether coordination will be needed between public safety entities and a D-block or C-block entity. Regardless, coexistence will be on an LTE to LTE basis. As such, both to and from the public safety broadband block, interference will be discontinuous due to the nature of LTE resource block allocations and power control. HARQ provides the same benefit with respect to adjacent channel interference as it does with co-channel interference. While sporadic outage may occur, HARQ allows the system to reattempt an interfered transmission thereby mitigating the coexistence impact. As such, IPWireless believes coexistence concerns are minimal between systems in spectrum adjacent to the public safety broadband block.

B. Public Safety Roaming on Public Safety Broadband Networks

We view the Commission’s proposed definition of roaming in (87) as being generally appropriate, however we suggest clarification that a roamer should be able to receive service from a fixed station, to avoid any implication of a requirement for mobile stations to provide roaming service, for example in the data equivalent of a talk-around call, as this is not yet standardized in LTE. Furthermore, in some scenarios of PLMN ID and HSS architectures that are being considered for national roaming, “subscriber” could be interpreted as being a subscriber on a national roaming network. To address these points, IPWireless propose the definition be amended to ““A mobile station receiving service from a *fixed* station or system in the public safety broadband network other than *its home network*”

In respect of the proposed categories of roamer, we suggest that this should be defined by the public safety community. Our reasoning is that LTE is capable of providing various levels of prioritization, and also assigning pre-defined priority to inbound roamers, and requiring these capabilities to be implemented should fulfill the Commission’s objective to ensure interoperability. However, the allocation of the levels of priority and any necessary categorization of roamers should be operational decisions for public safety.

IPWireless agrees that all 700 MHz public safety broadband users should be able to roam on all other 700 MHz regional public safety broadband networks, as this is the fundamental purpose of interoperability and should not be questioned. We also agree that networks should be required to admit different priority categories of public safety roamers, noting that the quality of service provided should be in line with the policies of the roaming network, and may differ from their home network priorities. Should the definition of Eligible Users be extended to include such users as utilities, it is reasonable that these may not be afforded the same automatic roaming privileges as first responders. The commercial and operational terms and conditions for first-responder roaming should be the prerogative of the public safety community, provided that they do not impose unnecessary barriers to roaming when reasonably required.

1. Prioritization and Quality of Service to Support Roaming

Priority and QOS levels for inbound roamers relative to normal users in the local or regional network will vary from area to area, according to local needs and mutual aid practices. For example the priority given to in-bound roamers for mutual aid in New York City may be very different to that of a rural county. Therefore, in line with our comments on “Public Safety Roaming on Public Safety Broadband Networks” above, IPWireless suggests that the support of specific roamer priority and QOS should be determined by public safety on a regional basis.

2. Applications to Be Supported for Roamers

We generally concur with the proposed “applications” for which roamer access should be allowed, although these might be better defined as “connectivity services”, per our comments on “Applications”. The Commission should clarify the definition of “field based server applications”: for example does this mean servers in the field connected to the LTE network via UE’s, as this would impact network and UE design depending on the throughput requirements?

3. Public Safety-to-Public Safety Roaming Rates

It is not necessarily valid to base roaming rates on commercial operators’ tariffs, as the service levels (e.g. throughput), QOS and coverage may be very different, and the cost of providing service to a roaming user will depend on the economy of scale, which may be lower or higher in a public safety network compared to a commercial network. Instead, IPWireless suggests that rates be based on a formula that

reflects such factors as the service level required / used by roamers, and frequency of use, relative to the cost of the network. Roaming rates need to reflect the following:

- a) The overall capital and operating costs of the network. With reference to IPWireless' comments under "Performance", if for example a roamer requires a higher cell edge rate (to support a particular application) than the host network requires for its own needs, then it is reasonable that the roaming charge reflect this.
- b) The priority and QOS assigned to roamers: If the level required by inbound roamers is disproportionate to that of users in the host system, charges should be able to reflect this
- c) Any special or additional coverage or service level required by the inbound roamer: For example if a Federal agency requires coverage of an area (eg a national park), then it is reasonable to expect that the roamer should share in the related costs.. This could be either by a capital contribution, an annual or monthly fee, or a per-use fee.
- d) Any other special service level that a roamer may require.

In consideration of the points above, and lack of clarity of funding for public safety broadband networks, we submit that it is too early to set roaming rates.

4. Volume of Roaming Traffic

At this early stage, when even home traffic on public safety mobile broadband networks cannot be predicted with any accuracy, IPWireless suggests that no meaningful estimate of roaming traffic can be made. Ultimately, this will determined by the applications used, the frequency of their use, and the nature of roaming operations.

C. Federal Use

2. Roaming by Federal Users

IPWireless comments on "Prioritization and Quality of Service to Support Roaming" and "Public Safety-to-Public Safety Roaming Rates" are intended to generally apply to Federal users as well as public safety roamers.

D. Testing and Verification to Ensure Interoperability

1. Conformance Testing

In 3GPP, Conformance testing is only applicable to User Equipment. The eNodeB and EPC is covered by Interoperability testing as discussed in the following section. As a supplier of band 14 user equipment for public safety, IPWireless intends to have devices certified by the appropriate certification body, be it GCF or PTCRB, noting that both of these organizations approve UE's against the same test scenarios developed by 3GPP.

The Commission is proposing that certification be required within 6 months of the availability of the PTCRB testing process. We caution that, it is possible that at that point in time there may be a backlog of band 14 UEs entering the test houses and the subsequent PTCRB process, which may make a 6 month deadline impractical.

In terms of "future testing", this should only be required for later releases of the 3GPP standards applicable to public safety LTE, and noting that many new features may not be mandatory or required for public safety. Depending on the scope of changes in future 3GPP releases, software-only changes should only require regression testing. With these points taken into account, IPWireless agrees that it is appropriate to require future testing to ensure ongoing operability, but this should be kept to a practical minimum to avoid the conformance testing process delaying the adoption or increasing the cost of such features which may be beneficial to public safety.

There is no formal industry process equivalent to UE conformance testing for network infrastructure (eNodeB and EPC). For commercial operator networks, the infrastructure, UE chipset and UE manufacturers perform private testing, for mutual benefit in creating a successful market.

As such, to require this for public safety would impose a huge cost burden on the industry, which would ultimately be borne by public safety. However, as virtually the same infrastructure used by commercial operators will be used by public safety, there is reasonable assurance of infrastructure compliance with 3GPP standards, and hence interoperability with PTCRB or GCF certified devices. "Self Certification" by vendors, as discussed in "Interoperability Testing" below should be considered.

To the question of which organization should "represent public safety at PTCRB", we suggest that representation should not be required: PTCRB certifies UE's that have been tested for compliance with

3GPP standards, and any changes required by public safety need to be made in the 3GPP UE test scenarios, not by PTCRB. However, we do believe there is a role for an organization such as PSCR to liaise with organizations such as NIST PSCR to facilitate timely certification of public safety devices.

2. Interoperability Testing (IOT)

The IOT that is performed for the commercial operator market on roaming interfaces is in accordance with requirements and standards set by the vendors themselves, and is not governed by any standardized test cases or formal certification. The difference between this and UE certification reflects the relatively fewer number of infrastructure vendors, and commercial operators can ensure standards compliance by their selected infrastructure vendors through commercial arrangements. Such IOT does not automatically take place between all possible combinations of vendor infrastructure, but only where commercially required.

This is a case where, to gain the benefits of the commercial LTE ecosystem, public safety should align with the practices in the commercial 3GPP market. This is a benefit of public safety choosing LTE: As infrastructure vendors to public safety will also be selling LTE to commercial operators, equipment supplied to public safety can be expected to be equally standards compliant. To require IOT between all infrastructure vendors as a precondition for supplying to the public safety market would impose significant costs and delays in deployment. Assuming there are say 6 infrastructure vendors to public safety LTE, then there are 36 IOT combinations. If each vendor's cost for their side on an IOT test is say \$1million, then the total cost is $36 \times 2 \times \$1m = \72million . Each test, including logistics time, may take approximately 3 months, to a total of $3 \times 36 = 108$ months of testing. Some testing would take place in parallel between different pairs of vendors, but this could still delay deployments by at least a year, and still be cost prohibitive.

Accordingly, IPWireless agrees with the comments of Motorola and Harris in the *Technical Public Notice* that a process of self-certification should be used, for the Uu, S6a, S8 and S9 interfaces. Commercial differentiation as suggested by the District of Columbia in the *Technical Public Notice* would not conceivably occur on roaming interfaces, because these interfaces are not an area where commercial differentiation is required, so there would be no reason for vendors to do this. Therefore this should not be a concern.

As discussed above, IPWireless supports IOT testing with self-certification on *inter-network* interfaces for roaming and interoperability between separate public safety broadband networks, regardless of

vendors. However, in terms of *intra-network* interfaces, we believe that it should be the operator's decision on whether or not to deploy a network from a single vendor or multiple vendors. Given that each network elements in the RAN, EPC, HSS and PCRF could theoretically be from a different vendor, the number of permutations to test could run into the hundreds if not thousands. Where commercial operators chose to mix vendors in a network, this is their decision, for which they bear the costs either directly or indirectly. To require IOT testing on possible every vendor combination within a network would therefore be prohibitively expensive, and risk further delaying the deployment of public safety networks.

If self-certification of inter-network IOT is employed, as proposed by Harris and Motorola and supported by IPWireless, then the question of laboratory facilities to perform IOT becomes moot. However, there may still be a valid role for NIST PSCR to assist vendors in IOT testing for the purposes of self-certification.

E. Other Matters Relevant to Interoperability on Public Safety Broadband Networks

1. Network Operations, Administration and Maintenance

Network Operations, Administration and Maintenance of an LTE network can be viewed in two categories (a) "Element Management" consisting of configuration, performance and problem management of the RAN and EPC network elements, and (b) subscriber management.

In IPWireless' view, element management should be the decision of the individual jurisdiction; whether to operate this in house, contract it to a vendor or systems integrator, or centralize management with other jurisdictions on a regional basis. Element management need not be difficult; a vendor or systems integrator will typically supply network infrastructure with default parameters set according to work normally works best in a network of this type, and then optimized based on local operator requirements, RF planning and drive testing. The operator is then able to perform "tier 1" problem and performance management without any more difficulty than running a LMR network, consulting the vendor or systems integrator where required for "tier 2" analysis and support for more complex problems

Subscriber management in an LTE network is effectively the management of databases on the HSS and PCRF. Once the jurisdiction determines its policies, for example on QOS, managing these databases is a routine task, no different to programming of radios in a traditional PMR network, except that it occurs in a different part of the ed-to-end system. Ideally, it should be the individual jurisdiction's decision on whether to manage the HSS and PCRF locally, contract it to another party, or participate in a regional or national HSS/PCRF. We note that this question is closely interrelated with how the issue of the limited range of PLMN ID's is solved.

3. Devices

120. Channel bandwidth requirement:

In the 3GPP standards, it is mandatory for a UE to support all channel bandwidths from 1.4 MHz through to 20 MHz, intended to facilitate international roaming between widely disparate networks. While this will not be the case in US public safety networks, where only 5 +5 MHz and potentially 10+10 MHz (including the D Block) are required, 3GPP compliant UEs will support the other channel bandwidths by default. The Commission therefore only need to mandate 3GPP compliance, and not specifically mandate each RF channel bandwidth option. However, to minimize costs and speed deployments, IPWireless suggests that only 5+5 and 10+10 MHz be required for any public-safety specific certification or interoperability testing.

121. Band Class 14 Support:

As the Commission has noted, 3GPP band class 14 includes both the public safety broadband spectrum and the D Block. To be 3GPP compliant, a UE must be able to work with channel bandwidths of either 5+5 or 10+10 MHz in band class 14, so there should be no requirement for the Commission to regulate this, beyond requiring 3GPP compliance.

122. Multiple Mode Support:

Many LTE devices will support fall back to 2G/3G standards, but this is not a mandatory requirement of 3GPP. For interoperability between public safety networks, only LTE band 14 support is required. Unless the Commission requires public safety roaming on commercial networks, IPWireless believes that this should be the individual jurisdiction's decision whether or not to purchase devices capable of 2G/3G roaming, and we expect this to be according to their local build out plans and budgets relative to commercial network coverage and the ability of commercial networks to provide the service levels and

prioritization required. While not specifically asked in this proceeding, this question also relates to UE support of other band classes at 700 MHz, that is band classes 12, 13 and 17. IPWireless believes that is desirable for a public safety UE to support these other band classes, but it should not be mandatory, especially considering some commercial LTE networks in the US will be operating in other bands (such as AWS, PCS and EBS/BRS), and it is not feasible to require all possible commercial roaming bands to be supported in a UE.

4. In-Building Communications

IPWireless agrees that in-building coverage for public safety broadband networks is highly desirable, and in most likely essential in the very long term as LTE becomes increasingly relied upon for mission-critical communications. However, this must be balanced with local requirements as well as the cost of deploying a network with in-building coverage. Our company has been involved in radio planning of 700 MHz networks ranging from the dense urban environment of major cities to rural environments such as Arizona, and most notable is the wide variation in requirements, based on building types and size, foliage clutter around buildings (which adds to the penetration margin required), and the types of user equipment to be supported. It is therefore very difficult to impose a “one size fits all” requirement without imposing an unnecessary cost burden on some, and potentially rendering a network unaffordable without guarantees of unlimited Government funding. Along with in-building penetration margins, the UE type (such as a handheld device) used in a building versus on a vehicle may have lower antenna gain, compounding the problem. In a hypothetical example comparing outdoor coverage with a vehicle mounted antenna of 3 dBi gain versus indoor coverage with a penetration margin of 12 dB to a USB Stick UE with typically -3 dBi antenna gain, the difference in link budget requirement is 18 dB. Therefore a network to provide indoor coverage will cost approximately 10 times more than vehicle coverage in this example. This is a clear illustration that, while indoor coverage is highly desirable, the cost impact and other practicalities must be fully considered.

As a reference point, we also note that the commercial 3G networks do not have consistent in-building coverage in all areas, even in the major cities, despite the huge capital investment of the commercial operators.

This highlights the need for “LTE Relay”, so that in-building coverage can be provided via “repeater” type capabilities in a vehicle parked nearby. This capability could provide coverage economically when and where required, avoiding the high cost of blanket in-building coverage across a jurisdiction. LTE Relay

capability is being developed as a feature of “LTE Advanced”. LTE Relay is intended to operate either out-of-band on a separate frequency to the donor (i.e host) eNodeB, or in-band, where the donor eNodeB allocates specific sub-frames for use by the relay eNodeBs, avoiding interference between the two. While the in-band option does impact the overall capacity of the donor eNodeB, this is dynamic and only has an effect when relay eNodeB’s are active, and is less of an issue if public safety gains extra capacity through the allocation of the D block. It is possible that a relay eNodeB in the overlap area between cell sites could cause interference to an adjacent site, which must be taken into account. (LTE relay deployments in commercial networks have the option of using different spectrum to avoid interference)

Longer term, as more funding becomes available and networks get progressively built out, we expect that in building coverage will increasing improve, as it does on the commercial networks, providing the level of in-building coverage required for mission critical communications. However, to reiterate, this requires substantial cumulative capital expenditure over time, and will cost many times more than the amount of Federal funding that is currently envisaged.

In consideration of the above, IPWireless does not believe that it is practical or economic to require 256 Kbps UL minimum data rate with indoor coverage to the first wall for all jurisdictions, as proposed by the commission. We submit that LTE relay is the most practical way of providing in-building coverage at incident scenes in the short to medium term

Distributed antenna systems are increasingly used by commercial operators to provide good in-building coverage in major buildings, shopping malls and campus environments. These are most often provided by the building owner, sometimes with a cost contribution from commercial carriers, and are usually multi-band to support multiple carriers. However, many existing systems do not support the 700 MHz band, and because of the adjacent channel coexistence issues that exist in this band, some systems may not support band class 14. IPWireless believes that the Commission should encourage distributed antenna vendors and building owners to deploy systems that support band class 14, and solicit the support of the commercial operators in this regard. It should be noted that such systems rely on building infrastructure in terms of power and cabling, which may not be available in a event such as a major fire or earthquake, and therefore distributed antenna systems are not a substitute for other methods such as LTE Relay.

5. Deployable Assets

IPWireless agrees that “cells on wheels” (“COWs”) can be valuable tools for an emergency response, and that public safety agencies should be permitted to deploy these where required. These may either incorporate standard eNodeBs, or Relay eNodeB’s as discussed in “In-Building Communications” above.

It should be noted that in a single frequency network (n=1 frequency reuse) as employed by LTE in the 700 MHz public safety spectrum, the deployment of COWs has to take consideration of interference management, in respect of other cells in adjacent geography, or other permanent cells providing coverage in the same geography. For backhauling of COWs, the options include:

- LTE Relay, where the COW acts as a LTE relay node off a permanent Public Safety network. The antenna on the COW connecting to the donor (host) network can be mounted high and/or utilize directional gain to allow it to operate at a distance from the host network and to achieve highest possible throughput through operating at a high modulation and coding step.
- Conventional point to point microwave operating in licensed bands.
- Point to point or point to multipoint technologies operating in the 4.9 GHz public safety band, but noting that some of these technologies may not be able to support the throughput required by a 3-sector LTE eNodeB.

Where the Commission asks about “satellite bands for backhaul”, it is not clear whether this refers to using satellite services for backhaul, or simply using spectrum allocated to satellite on an auxiliary terrestrial basis. In the case of using satellite services for backhaul, high latency and capacity limitations should be taken into consideration.

Furthermore, COWs can be deployed using a small scale EPC / HSS / PCRF located within the COW itself, allowing totally autonomous, or semi-autonomous operation. In this scenario, low capacity satellite backhaul could be optionally used for remote HSS authentication, where the high latency of satellite connections would have less impact.

6. Operation of Fixed Stations and Complimentary Use of Fixed Broadband Spectrum

IPWireless supports allowing fixed services in the 700MHz band on an ancillary basis, but only as part of LTE networks, and not through use of the spectrum for other fixed technologies.

Our experience with deployed public safety broadband networks shows that fixed UE stations should not create undue interference. For all users, interference, particularly on the uplink, is managed via power control. Though the specific implementation is vendor specific, power control in principal accounts for and avoids interference at the cell edge by calculating each UE's relative geometry, difference in path loss between serving cell and neighboring cells, power control applies equally to fixed and mobile stations.

As such, the demand for support of a limited number fixed stations by public safety agencies can be met by the LTE mobile broadband network without degrading network performance. Fixed stations will contribute traffic loading to a network, especially if used for video services, but operators can manage this along with mobile applications in their traffic planning and management of prioritization.

8. Public Safety Broadband and Next-Generation 911 Networks

IPWireless recognizes the value of increased situational awareness brought about by pushing the data associated with NG911 out to personnel in the field. While we not familiar with the exact nature of the implementation of NG911, our understanding of NG911 is that its fundamental goal is to drive towards an IP-enabled emergency network using open standards. Given the inherent capability of LTE to carry IP, NG911 data can be carried over the network. However, IPWireless does not comment on the higher layer transport and security aspects required to enable connectivity between LTE users and 911 centers.

F. Section 337 Eligible Users

As a supplier of mobile broadband systems to New York City and Gillette Wyoming, IPWireless is acutely aware of the benefits of "multi-agency" networks, where the network is shared between first-responders and other city / county agencies on a relative-priority basis, and operating in license spectrum where the type of usage is not restricted. The primary benefit of multi-agency networks is through the economies of scale and scope in sharing the cost of a capital-intensive network, but also in increasing the breadth of funding sources, such as Federal and State grants for a variety of services to the public, beyond just Public Safety.

A multi-agency network is made possible by the ability of a LTE network to very efficiently share capacity on a shared-channel, packet-switched basis. A typical 100-site LTE network can deliver around 2 gigabits/sec of usable downlink throughput in the Public Safety 5+5 MHz spectrum, increasing to 4 gigabits/sec if the D Block is also allocated to public safety. In a major emergency or disaster, public safety may need all of the capacity that an LTE network can deliver, particularly on cell sites covering an incident area. Extensive use of video services on the network can also increase public safety's demand for capacity. However, in some (but not all) networks, significant capacity will be unused at times where major incident responses are not in progress, or on parts of the network not involved in such responses. We believe it is both in the public interest, and in the interests of efficient use of the 700 MHz spectrum asset, for other public agencies to be permitted to share in such a network on a secondary basis. IPWireless goes further, and suggests that this will in many cases this will be essential to the basic economic case for a network to be built, especially a network that is able to provide the coverage, building penetration and data throughputs that public safety ideally desires.

The priority and quality of services mechanisms defined in the 3GPP LTE standards provide an effective mechanism to ensure that, in a shared multi-agency network, first responders get absolute priority and network access and capacity when they need it, that need being defined by public safety. In this way, non-public safety users can be secondary and preemptible.

In the interests of facilitating the deployment and operation of mobile broadband networks for the primary benefit of public safety, IPWireless proposes that the Commission broaden the definition of eligible users to allow use a network operating in 700 MHz spectrum allocated to public safety to include all local, County, State and Federal users, as well as regulated utilities. However, we propose that inclusion of such non-public safety users should be at the discretion of the public safety operators in each region, according to their local situation. We note that the public safety entity that would need to make this decision needs to be defined by the Commission and/or the PSBL. Via the mechanisms described, we believe this proposal maintains compliance with the Section 337 language regarding "principal purpose" since the system can be configured such that any non public safety users will only be given access on a purely secondary basis without degrading service for the "principal purpose". The exact nature of the secondary basis needs to be defined by the public safety entities or PSBL.

We believe that sharing of 700 MHz broadband networks between public safety and other government agencies and utilities will make efficient use of the allocated spectrum, increase economies of scale and service the public interest, without the need for the network to provide services to the general public.

Respectfully submitted,

By:

Roger Quayle

Chief Technology Officer

IPWireless