core, and on this diagram I have showed some key elements of that which I'll go into a little bit more detail. This is the place where ultimately public safety would be able to innovate on the enablement of new applications. It's the place where public safety would authenticate its users and ultimately manage access to its applications and services. It's also the place where public safety would arrange and implement roaming agreements between networks.

So the core network's incredibly important. Given the uniqueness of public safety's applications and services, it would seem that having a unique core that public safety can work with and manipulate and develop would be a tremendous advantage. That said, it is not inconceivable in situations where the public safety entity is maybe smaller in scale, that those services applications may be hostable on the commercial service provided by a commercial carrier, and that that's well within the boundaries of possible with technology we have today.

The second key element I want to talk specifically about the most expensive part of this endeavor, the access network, the very large preponderance of money and investment to ensure reliable coverage would have to be invested in access

network infrastructure. It's quite clear even at 700 MHZ that the quality of coverage that would have to be laid down in the ground throughout our cities, in rural areas, and in the parks and beyond, would have to be of such a quality to support ultimately voice and video services, that many thousands of towers would be required to achieve that goal.

Not withstanding the fact that existing public safety infrastructure would be complementary to that within the major metro areas, I think the FCC's estimate of 41,000 nodes is a very reasonable estimate, you know, to deliver the kind of performance that public safety is looking for. The required investment to make that happen in terms of cell site locations, hardened E-node Bs, which would be the bay stations, the antenna subsystems, the powered backup, and backup systems required to deliver the reliability that public safety and commercial operators both strive to achieve, is a significant investment and both in terms of complexity and cost.

So in terms of common goals, there is an opportunity to align requirements on reliability as both commercial and public safety operators strive to improve reliability of their systems for their constituents. The third element that I'd like to

address today is this aspect of a transport network. We know from experience at T-Mobile through implementations that we've made in international countries such as Austria and Slovakia and the Czech Republic where we've built broadband access networks over the last few years, we know that the transport network is a key element to delivering on the LTE performance promise.

And by saying that, it's simply more than just a fiber connection to the cell site, but includes beyond that complex architectures that must be supported between access nodes and E-node Bs, and performance figures which are by any measure quite difficult to achieve. We have practical experience of that in the ground, we've measured it, and we have a good understanding.

We believe the commercial carriers who are currently working with LTE and perfecting it will bring tremendous value in a collaboration with public safety and derisk what traditionally has been one of the simpler parts of any wireless network, the transport. And we know from a TDM world, the circuit switch world, that transport was quite manageable. In this new world of LTE it is quite a challenging and difficult architecture to make practical and

deployable. So that's the aspect of IP transport.

The scalability of that transport network to deliver video services and voice in the future is a significant investment in itself and requires many points of presence throughout the country to ensure a national footprint, and adequate bandwidth through time to accommodate scaling as new services are added. So with that, I'd like to move on to address something else rather important to the aspect of sharing infrastructure.

The question of security and the way in which that would be handled in this shared infrastructure concept is absolutely key to giving public safety the kind of confidence it might need to enter into sharing agreements. I think it's important to recognize that LTE inherently has very high standards for security at the lower levels, which includes ciphering at the physical layer and authentication mechanisms which are much stronger than today's 2G and 3G networks, or I should say even stronger.

And that's an important aspect of providing some fundamental security and user authentication end to end. Now, notwithstanding that, there's certainly this aspect of enabling secure tunnels between public

safety devices and/or commercial devices where the secure tunnel using technologies such as IP SEC, which is standardized in 3G PP, to connect to secure servers within the public safety core to ensure end to end secure tunnel transmission. And that technology again has been commercialized broadly, and we at T-Mobile use it to support many of our services today.

So end to end security using IP SEC, and it's important to recognize in that example I've given public safety would be able to have control over the two end points both the device at one side and the authentication and security servers within the core network. So control of security is well within reach even though infrastructure may be shared. Moving on to build and some of the insights provided by Patrick earlier.

With respect to quality of service management, I think it's fair to recognize LTE was architected in this concept of end to end quality of service management, such that operators could regulate bandwidth as it was allocated to different services to differentiate between real time services, best effort services, and background tasks. And that foundation builds a very rich feature set of controls within LTE and the IMS core to manage and regulate bandwidth.

What I've laid out in this chart is a very high level concept of how wireless priority service may work and how bandwidth regulation could work in a shared asset situation. Policy control affected through policy control functions on both public safety core and the commercial operator core, and made possible by a unified set of quality of service classes that would be agreed through standards -- and they are in process of being standardized through the Getz initiative.

And then bandwidth regulation on the carrier side to ensure that if bandwidth needs to be set aside and prioritized for public safety services under a roaming situation or a hosting situation, that that bandwidth regulation creates space for the importance and high priority public safety traffic. So that's a very high level view of how we at T-Mobile see quality of service operating in a future core, and I want to thank you for your time today to listen to my presentation.

MR. KNAPP: Mark, thank you. Turn the floor over to Dale for his observations on some of the things we've talked about.

MR. HATFIELD: Thank you, Juli. First of all, I want to congratulate of course the Commission

and Admiral Barnett and his staff and the National Broadband Plan team for, well, not only just for what they've done in public safety but for what they've done in terms of broadband for the nation in total. I've just really been impressed with the quality of the analysis, the being fact based and so forth, so I think it's just a tremendous, tremendous job, and while some of us may disagree with some of the things at the edge, overall I think just a tremendous, tremendous job and I really do commend them for it.

I probably should say that my affiliation at University of Colorado at Boulder, I direct the Silicon Flatiron Center, and I probably ought to say that I'm appearing here today as a private citizen, my comments are my own. As Juli indicated, I've been asked to sort of respond to what I have heard, I didn't have a presentation but rather I was to respond.

And I'm not sure exactly where to start, but in my own thinking one of the key things that I've learned from listening to discussion here today and reading some of the material that have been filed is that we have a real problem in public safety because of the need for a very intense, to meet very intense demands at a particular location. In other words, you

may need a lot of video signals at one time, and that creates a need for a spectrum perhaps beyond the 5 by 5 that public safety has there now.

I guess having been around the spectrum management business for an awful long time, I guess what concerns me there is that we not let that sort of requirement drive spectrum allocations in such a way that we end up with spectrum that remains idle most of the time. In other words, to meet a peak, what we have is a situation where we may have a very intense peak and if we set aside spectrum to meet that peak, most of the time and in most locations that spectrum would be idle.

And what that leads me to, and perhaps I'm stating here the obvious, what that leads me to, again from a big picture standpoint, is just the critical importance of sharing. We heard Mark talk about sharing in both dimensions, one of course is to reduce the cost of network, but the other is to make sure that we use this vital resource, the radio spectrum, in an efficient way. So that leads me to the importance, this peak problem, leads me to the importance that we must focus on sharing, and I'm talking about spectrum sharing.

And of course that immediately leads you to

the notion, as has already been expressed, that the sharing sort of going in both directions, both commercial users being able to use public safety spectrum when the public safety entities are not using it, or in times of one of these real peak things of being able to get traffic from the commercial sector. So it all comes back to sharing.

And then to me, what I think is the good news from a technology standpoint is it really looks like we have the technology to support that sort of sharing. The signaling network and so forth we've talked about here, they've gotten so much more powerful than the days when I was teaching, you know, basic circuit switch telephony and the very limited signaling networks.

We really have powerful signaling networks that can enable us, I think, to do the sort of sharing that needs to be able to manage the spectrum more efficiently. And by saying that I don't mean to say that there aren't important control issues that have to be resolved, but from what I can tell and what I've heard here this morning, I really believe in LTE that there is the capability, the coming capability, to be able to handle very dynamic forms of sharing from a technical standpoint.

So I have a lot of confidence that we can do it technologically and not end up with a situation where we have a lot of spectrum that sits idle most of the time, especially a spectrum as we all know here at 700 MHZ which is so darn valuable, having it sit idle is a terrible waste. Thinking about other things, I thought perhaps, my own reaction here this morning, is a little bit -- I'd personally like to hear a little bit more about the mission critical voice situation and how over time we can migrate the mission critical voice from the existing generally P25 networks, if you will, over to this new architecture.

I think there are some real challenges there, and I think as a country we have probably some challenges in trying to maintain and increase the interoperability of that voice network at the same time we're making the necessary investment in the broadband data area as we just talked about. I would say one thing I think that's important that's both bad news and good news.

The bad news is that a lot of this capacity requirement seems to be driven by video, it sort of overwhelms voice when you look at it in terms of capacity requirements. And that's sort of the bad news because it's putting so much pressure on our

spectrum resource to be able to handle video. The sort of good news is though that you can maintain the basic voice capabilities to do the 911 calls and things like that because they're so much less bandwidth intensive and you can shut down I believe, preempt if you will, some of the less critical video requirements, what I'm talking about here is consumer type video requirements, and free up an awful lot of spectrum and maintain spectrum, free up spectrum for maintaining basic voice connectivity.

But here again the issue to me is sharing. If I had one message to convey from what I heard is the critical importance of sharing, and of course that leads then to the next issue of making sure we develop the control structure and so forth that allow sharing across this boundary between the commercial side and the public safety side. So that was my major, there are some other things here probably in the details that we might be interested to comment on, but I think those are the two critical points that I took away.

MR. KNAPP: Thanks, Dale. I just know I'm going to ask somebody's favorite questions. One of the issues of concern, Robert, you touched on this, to public safety is coverage. And often the demands and the spectrum demands go to the question of the

coverage at the edges of the cells. And although LTE is still a developing technology, is there anything that can be said that will help with the next generation of technologies in improving the data rates that are available at the edge of coverage? I know we heard a little bit before about relays and so forth. Does anybody want to tackle that one? Mark?

MR. MCDIARMID: So cell edge data rates, yes, the challenge obviously being having a good enough signal to noise ratio at cell edge. We know from 3G and CDMA that the cochannel nature of those CMA systems really doesn't give you the cell edge performance that you really desire compared to OFDM based systems, so we know that LTE is going to be a lot better.

That said, some of the measurements we're taking in our network in Austria are showing tremendously, you know, robust signal strengths and, you know, delivering robust throughputs, certainly enough to meet the public safety requirements that we're seeing here today. So I think there's encouraging signs from the technology, and obviously as investment and the ecosystem picks up we're going to see investment in things like interference cancellation, and I think that was mentioned in the

panel already. So I'm optimistic maybe on that one.

MR. KNAPP: Go ahead, Robert.

MR. LEGRANDE: I'm a little less optimistic, because, you know, in public safety, guys, we have to design for worst case. We can't design for best case, we can't even design based on the commercial premise. If you drop a commercial user it's a lot less tragic than if you drop a public safety user. So when we talk about cell edge coverage, I don't disagree with you that there has been advancement, certainly, you know, having, again, launched that valerian network that was an OFDM based network, you know, we had a lot of problems quite frankly with dropped calls or dropped signals and, you know, that was one of the complaints coming back from the field is that they would be going along, they would, you know, almost be green with coverage then all of a sudden it drops to near zero.

So, you know, in a public safety environment I think we're making a lot of assumption that it's going to almost mirror the commercial environment, will it be okay to see that degrading signal towards that, and that's not the case. I think we need to assume that public safety has to have solid coverage, we have to assume that we cannot lose connectivity, we

have to assume that we cannot drop any packets, and we have to design and allocate spectrum based on that.

MR. KNAPP: Patrick, do you have any thoughts on this? I know you talked about the relays a little bit.

MR. RINGQVIST: Yeah, no, I agree with Mark's statement earlier, that we do see a significant improvement from an LTE point of view over 3G technologies when it comes to cell edge performance. And of course cell edge performance is a key issue not just for public safety but also for commercial, and therefore there are a lot of activities going on on how to improve the performance at cell edge.

So yes, I mentioned too those technologies that are being addressed right now in the standards bodies, interference cancellation techniques by through the coordinated multipoint technology as well as relays. And both of those technologies can be used to improve performance at cell edge. So I do see that there are improvements on the horizon, I think we still need to understand a little bit better what exactly is needed from a public safety point of view, and maybe there are some of these things that we need to implement before we can get to a truly mission critical network from a public safety point of view.

But that shouldn't stop us from starting. I think that's the main message, we need to start and keep going.

MR. KNAPP: Open -- go ahead, Roger.

MR. QUAYLE: If I could just make a further comment. You know, we've talked about the benefits to public safety of using LTE and being able to capitalize on the ecosystem. Another dimension of taking advantage of the 3G PP ecosystem is that I think it's recognized in 3G PP that with any technology, increasing cell edge throughput is a challenge.

And I know that a lot of effort is going into improving cell edge performance amongst the 3G PP member companies. But what you have in 3G PP with the vendor community that's behind it is really the best wireless brains in the world looking to solve these problems. The technologies that are generally used in LTE now to deal with intercell interference and cell edge performance are really interference avoidance. One of the areas that my company has a lot of experience in is true interference cancellation. Now, that is more challenging with an OFDM technology, but I think if you give it a few years that is going to be solved.

MR. KNAPP: Open the floor to questions from my colleagues up here on the panel. John, Stagg, Walter? This is a first, that I don't have questions from these three people.

MR. JOHNSTON: I don't have a question, but let me add something about coverage.

MR. KNAPP: You want to pull the mic over, Walter?

MR. JOHNSTON: I think, you know, traditionally public safety networks have sought to conserve cell sites or conserve radio sites and get maximum coverage out of a single site, whereas commercial carriers because they're trying to go for spectrum efficiency have built more cell sites, and they have learned that with coverage issues more cell sites is better.

So the plan that was put forward assumes that the money is allocated to upgrade the maximum number of commercial sites, and I think that's a big improvement in performance that public safety would see over a traditional public safety build. So we're not building, you know, range limited, coverage limited sites, but especially in metro areas, we're basically going with a commercial model with, you know, a much larger number of cell sites. And I think

that performance in general will be improved over what could be afforded by public safety.

MR. KNAPP: Stagg?

MR. NEWMAN: I agree with Walter. I've got first an observation on I think a very valid point that Robert raised, and then a question raised by another point he raised. Certainly our model envisions, and I should have made this clear, using both commercial and public safety assets, and that's the beauty of the local RFP process because it can be tailored to the local situation.

Let me be very specific about that. Two states that are about the same size, Kansas and Missouri. Kansas has built out, I think it's 800 MHZ LMR network, so they have like 400 LMR towers throughout the state that could be a very good asset for building out particularly in the rural areas a broadband public safety network that could be brought to the partnership. Missouri, same size but they chose to build out a VHF network, so they have 150 towers, so far fewer assets, so there it probably is more important to use commercial assets.

You know, New York City, they, you know, if they had built out a 700 network on their own they probably could only do 2 to 300 cell sites, but if

they partner with a commercial operator and each operator probably has a thousand cell sites in New York City, far more cell sites. So I think Robert's exactly right, it's bringing all the assets to the table to find the best economic solution.

Now, a question that Robert raised that I'm going to toss to probably Patrick and Mark and Roger may want to address it too, Robert made the very good point that if we have priority access on the commercial network in the times of an emergency, we need to make sure public safety packets go to the top of the queue, as I understand in LTE network that's not a real issue, that happens immediately, but you've still got to make sure that the 911 calls from the consumers go through, at the same time you don't want to see your bandwidth eaten up by the video gamer. So could you all say a little bit more about how you envision addressing Robert's question of how do we make sure when frequently you have an incident it's also when you get a peak in commercial traffic and how that would be handled?

MR. RINGQVIST: Yeah, I can start. So the priority scheme and the quality of service enablers that we talked about earlier in LTE, that enables a differentiation both between services and users. So

911 calls will get a certain treatment and certain differentiation, and so will cam public safety users as well. So depending on the schema that was agreed upon between the public safety operator and the commercial carrier, then you can define a schema where the place the 911 calls appropriately with the public safety calls and the reserve bandwidths for each category.

There are also ways where you can limit so certain type of traffic don't take all capacities, you limit so it still has some guaranteed bandwidth for other users. So there's a rich set of features available to you in order to build these type of networks. Let me also comment a little bit about the coverage issue before. So I think that when building a cellular mobile broadband network, like you're talking about here with LTE, is a different exercise than building a land mobile radio network.

Typically it's a compromise between capacity and coverage, and you really need to understand your traffic profiles and your coverage needs when building these networks. I would put forth that the commercial carriers have a lot of experience in this area on how to build a network using these cellular technologies, and a partnership with a carrier could certainly help

public safety understand on how to build a cellular type of network like LTE with better performance, meeting both the coverage and the capacity needs. So I just want to put that forth.

MR. MCDIARMID: Thank you, Patrick. Just to add a little bit, and I certainly agree with all your points. I think the key thing to remember, you know, a typical video stream from a, you know, a web service today may be several hundred kilobits per second in its data rate, and yet an important critical 911 voice call or a public safety communication voice call may be somewhere in the range of 8 to 12 kilobits per second.

So the simple action of regulating video usage and web browsing during times of emergency or need, the technologies to achieve that goal are designed into LTE and certainly we're beginning to explore how they're used. So that I see a lot of opportunity in terms of regulating bandwidths in a way that say in 2G and 3G was maybe not quite so rich as we'd like it to have been.

MR. LEGRANDE: So --

MR. KNAPP: Of course.

MR. LEGRANDE: It feels a little lonely up here.

MR. KNAPP: I've felt that way often.

MR. LEGRANDE: So many comments. So the first one is just kind of a piggyback on -- no, let me just start, let me rearrange the conversation a little bit around the past two questions. Let's just make a quick agreement, one agreement that in a world where public safety has 20 MHZ of spectrum it's going to better than a world where public safety has 10 MHZ of spectrum. So all the tools and things that we're talking about, which we're going to have to have regardless if we have 20 or 10, it's important for us to follow the same approach to make sure those are operationally at a level where we can trust them, okay?

So the argument isn't necessarily whether or not it's going to be better or worse, I think we, you know, all can agree as the geeks up here, that it's better to have 20. And now, as it relates to getting there, I think, you know, the thing that cautions me, I've got a little bit of experience with working on nuclear attack submarines and missile systems, and then, you know, since that was hard enough, I went to the District of Columbia.

So, you know, those first responders, when you interact with them, they see the ugliness of the

world, the most ugly thing that you don't want to know about, these guys see on a daily basis. Helping them to clean these things up or prevent those things, there couldn't be a more important thing that we do right now. I don't distrust technology, I'm a technologist -- as my kids would say, certified geek, don't talk to dad -- but at the same time I have learned enough through my years of technology that there are certain things that you have to be very careful about the introduction of technology in an environment like this.

So I don't disagree with anything that the panelists are saying other than the fact that it would be in public safety's best interest to be in the best position to provide the best tools. That is our goal, that is our mission, and that's what APCO is about. So that's my whole statement as it relates to yes, yes, yes, yes, yes, but this is better than that.

MR. KNAPP: John's been itching to grab a mic. Go ahead.

MR. PEHA: I was going to add something similar to Stagg. But also curious, Mark raised some important security issues, maybe others will have thoughts too, but you're talking about authentication protocols and IP SEC and the like, people may be used

to thinking about how that works within a network that they entirely control. If we're also talking about roaming onto commercial network and still wanting to make sure that both, you know, devices are properly authenticated and protected from eavesdroppers et cetera, are there any issues in that context?

MR. MCDIARMID: Yeah, very complex subject so let me try and chip away at that a little bit, John. I think first it's important to recognize that today commercial networks do carry secure traffic through tunnels reliably, and certainly at security levels that are deemed to be good enough for day to day use, right, so there's never so much -- more security is sometimes a good thing, sometimes a challenge.

But we have in our network at T-Mobile today secure tunnels running for customers, and they control how those tunnels are secured to a large extent, and that's a technology that provides -- and this is a very important point -- I think in a shared infrastructure model, I mentioned this earlier, you know, the old model of if I own the infrastructure I have absolute control, that was true then, still true today. If I don't own the infrastructure today but yet I have control over the end points and the tunnel

and I know the tunnel will be treated fairly in terms of bandwidth, then I still have control, I just don't need ownership.

And I think turning it around a little bit and saying, ensuring that the security levels are appropriate for public safety to use and finding and applying investment dollars to make sure those things are really the way public safety need them to be for the applications they wish to run, should be the focus of where public safety places its investment. The matter of coverage and coverage reliability and how those services are made reliable in the environment is the specialty of wireless carriers today with things like broadband services.

And I wouldn't say we're experts, but we're beginning to learn and master some of those skills. So there is a yin and a yang to this, the benefit of not investing heavily in access networks or in cell sites where not needed, and sharing where opportunistic, allows public safety possibly to apply its dollars more productively in things that really do make a difference.

MR. KNAPP: We've got about ten minutes, and I wanted to give an opportunity if there's some questions from the floor, just step up to the mic and

not have a real long line. Yes, if you could say your name and introduce.

MR. LABOUE: Yeah, Jerry Laboue from Sage Alerting Systems and also the Society of Broadcast Engineers. As many of you know, the same public service, Public Safety and Homeland Security Bureau that is taking care of this broadband project very nicely I would say, is also working on the modernization of the emergency alert system, the technology that gets emergency messages out to the public, whether it's amber alerts or the President's national messages or whatever.

We have as Sage, Society of Broadcasting Engineers and others, petitioned the Commission for a sliver of spectrum in the 700 MHZ D block, which would be used exclusively for the back channel for the emergency alert system on the national, local, and statewide basis, and I wanted to bring that to everybody's attention and I hope it gets some support. We just filed another comment in the second further notice of proposed rulemaking on EAS again requesting just a tiny little bit of spectrum, but clear spectrum that could be used for broadcasters, radio, TV, cable, and emergency management, and we think that's in keeping with the spirit and the idea of the D block.