UNITED STATES
FEDERAL COMMUNICATIONS COMMISSION

IN THE MATTER OF:)
)
700 MHZ NATIONWIDE INTEROPERABLE)
PUBLIC SAFETY WIRELESS BROADBAND)
NETWORK WORKSHOP)

Pages: 1 through 94

Place: Washington, D.C.

Date: March 17, 2010

HERITAGE REPORTING CORPORATION

Official Reporters

1220 L Street, N.W., Suite 600

Washington, D.C. 20005-4018

(202) 628-4888

contracts@hrccourtreporters.com

IN THE FEDERAL COMMUNICATIONS COMMISSION

IN THE MATTER OF:	)
	)
700 MHZ NATIONWIDE INTEROPERABLE	)
PUBLIC SAFETY WIRELESS BROADBAND	)
NETWORK WORKSHOP	)

Commission Meeting Room
FCC Building
445 12th Street, S.W.
Washington, D.C.

Wednesday,
March 17, 2010

The parties met, pursuant to the notice, at 9:32 a.m.

BEFORE: JULIUS KNAPP, Chief, Office of Engineering and Technology, FCC

ATTENDEES:

JAMES ARDEN BARNETT, Jr., Chief, Public Safety and Homeland Security Bureau
STAGG NEWMAN, Chief Technologist, National Broadband Team
JOHN PEHA, Chief Technologist, FCC
JENNIFER MANNER, Deputy Bureau Chief, Public Safety and Homeland Security Bureau
WALTER JOHNSTON, Chief, EMC Analysis Division, Office of Engineering and Technology

APPEARANCES: (Cont'd)

Presenters:

ALLAN SADOWSKI, Information Technology Manager, North Carolina State Highway Patrol

ROBERT LeGRANDE, II, Former Chief Technology Officer, District of Columbia Government, President and Chief Executive Officer, LeGrande Technical and Social Services, LLC

PATRICK RINGQVIST, Vice President, Wireless Network Solutions, Ericsson, Inc.

ROGER QUAYLE, Chief Technology Officer and co-founder, IPWireless, Inc.

MARK McDIARMID, Director, RF/RAN Systems Engineering, T-Mobile USA

DALE N. HATFIELD, Executive Director, Silicon Flatirons Center, University of Colorado at Boulder

P R O C E E D I N G S

(9:32 a.m.)

MS. MANNER: Good morning, everyone, welcome to the 700 MHZ Nationwide Broadband Public Safety Wireless Network Technical Forum. What I'd like to do is welcome you this morning, welcome our panelists, and introduce Jamie Barnett, the Chief of the Public Safety and Homeland Security Bureau.

MR. BARNETT: Jennifer, thank you, and thanks to all who have made this possible. Thank you for being here, and especially to our panelists today. Just a couple remarks before we start. We were excited about having this, the panel, since really there has not been much going on here at the Commission for the last few weeks and months and we needed some excitement.

Actually, with the delivery of the broadband plan yesterday, while that may be a culminations in some ways it's actually also a beginning, and we are excited about it, you've seen the amount of comments that are coming in, there's a lot of excitement about it. One of the ones that I'd like to highlight to you, and they're coming in from the Congress as well, but the President himself made comment.

And I'll actually quote him here, "My

Administration will build upon our efforts over the past year to make America's nationwide broadband infrastructure the world's most powerful platform for economic growth and prosperity, including improving access to mobile broadband, maximizing technology innovation, and supporting a nationwide interoperable public safety wireless broadband network."

It's good to have the President, Commander in Chief, recognize that and say that he supports that, and gives me great hope for moving forward. With that, I'd also like to make announcement this morning, because the broadband plan also maps out a great deal of work for the FCC. Today as one of our very first actions following the release of the National Broadband Plan, we'll be issuing a public notice seeking comment on the NPSTC Broadband Task Force recommendations as submitted to the Commission by the Public Safety Spectrum Trust.

We'll be seeking input concerning these recommendations that address the technical aspects of interoperability of state, local, and regional deployments that are the subject of pending waiver requests. Our intent is to determine the extent to which these recommendations could form the basis for action on these waiver requests, including technical

and operational requirements for the Emergency Response Interoperability Center and what it would adopt.

The comments date for the interested parties is April 6, I believe, and then the deadline for reply comments is April 16th. Following the receipt of comments, we'll move quickly to act by early to mid summer on the waiver requests to that those agencies seeking to deploy public safety broadband networks will have the initial set of requirements necessary to pursue any desired partnerships in network deployments.

At the same time, I'm glad to see that NIST and NTIA through their Public Safety Communications Research Program are seeking participation in a demonstration network for the public safety broadband communications in the 700 MHZ band. We believe that this demo network would complement the FCC's overall efforts for ensuring that first responders have access to a nationwide wireless interoperable broadband public safety network, and including action on these waiver requests.

So some of you have heard me say this before, but I certainly want to emphasize it now. When we took this on, there were a few requirements

that I asked the team to look at. Number one, it was going to be fact driven, data driven from the very beginning, we would base our decisions on that, and we would look at everything. And so at one point we had some 27 options on the table that got narrowed down to what we think is the best plan to move forward.

What I told them is, the plan is going to have to be truly nationwide, it has to extend from the densest city down to the most rural area in America. It has to be truly interoperable, that is the overall goal that we have to have. And it has to be viable, both from the economic standpoint that companies would want to partner with public safety agencies, public safety agencies would be able to afford this, but also that it would be viable from a technical standpoint, which brings us to today.

Now, there has been a lot of debate and obviously a lot of concern about the D block, and you'll get to hear about that and ask questions about it as well. One thing that I think is interesting -- and I got to see all of the presentations that you'll see today -- one of the things that I would emphasize are the areas of what I would call growing agreement on.

So I mean I think everybody agrees that we

need to have a nationwide and interoperable network, but I think you'll see there are some other areas of agreement, such as that we need funding for this, because truly it will not be nationwide and it probably won't be interoperable unless we have some public funding for this. And the plan puts forth some very I think innovative ideas about moving for that. We have to have funding, we have to start talking about that we need funding, and you'll see that today.

There are also some areas which you might say of concern that I think you'll hear about today, and that's the roaming and priority access. I have that concern too. That's why the plan actually maps out that we are going to have a very intense program of making sure that we get priority access and roaming right, and so that's fair game today and we want to talk about it. Once again, thank you for being here, thank you, panelists. And I'd like to turn it over now to our Chief of the Office of Engineering Technology, the one and only Juli Knapp.

MR. KNAPP: Thank you, Admiral Barnett. Welcome, and happy St. Patrick's day to all of you. In keeping with St. Patrick's day we are hoping today to have a robust discussion followed later on in the day by a robust celebration. Yesterday was truly

exciting for the Commission in rolling out the National Broadband Plan. The public safety piece of that is one of the most important and vital parts of the plan.

And for the engineers, as exciting as yesterday was, today when we get down and start talking about the nitty gritty details of the technology, that's what really turns on the engineers. So we're going to kick off the day with a presentation by Dr. Stagg Newman, who is our Chief Technologist in the National Broadband Team, and Dr. John Peha, who is Chief Technologist of the FCC. John and Stagg?

MR. NEWMAN: Thanks, Juli. I've got the easy part, I do the first two charts and then hand over the technical work to John. Maybe in keeping with the theme of St. Paddy's day, one of the challenges that we had to answer from Admiral Barnett was the green challenge. And in this case, green means making it affordable, green as in the color of money as opposed to the energy green.

So what we've tried to do is come up with a plan that we think cost effectively uses the commercial assets our there but give public safety their own spectrum for their core use and takes advantage of all the different ways to meet their

needs. If you look at the requirements, you know, high performance uplinks, high capacity, performance inside buildings, and performance in wilderness areas and remote areas, there is no way you can build a single network architecture to meet that unless you can afford to put out literally, if you tried to meet all those requirements with a single network build, hundreds of thousands of cell sites and you'd have to go to Congress $50 billion, $100 billion.

That's not going to happen unfortunately in this environment. So we've tried to look at all the things that go into a network architecture. If we could flip to the next slide please? Thanks. And say, how do we come up with a total plan to meet public safety's needs? So we came up with what we are calling the pyramid chart. Light up the public safety broadband spectrum, 10 MHZ. Give them their own radio access network but use commercial assets, and give public safety on a local basis the choice to choose a partner.

They may choose a current cellular wireless operator, they may choose a new D block operator, a new systems integrator, that's their choice, but use the commercial sites that are out there, the back haul that's out there, leverage off all that. Okay, so

that's the core day to day public safety broadband network using 700, which has, you know, great propagation characteristics. Now, there will always be times when you don't have enough capacity. I don't care whether you have 10 MHZ, 20 MHZ, if you truly have a Pentagon type disaster or a Katrina type disaster, you need more capacity.

So for those true dire emergencies, do a priority wireless broadband service. You'll hear a lot more from John about how that works, but the good news is in a modern IP world, you can have the type preemption priority et cetera you need so public safety truly gets the priority they need. The 911, you know, consumer calls can still go through, but, you know, people aren't doing video games in a dire emergency. You know, same technology that's used in the military to make sure for example admirals have priorities over generals in an emergency. Moving on.

(Laughter.)

MR. NEWMAN: Okay, but we've got another problem, how do you get deep inside buildings? You know, large commercial buildings where either you may have very high populations in an emergency and certainly you can't get a signal that's from an outside distant antenna deep inside buildings, as we

all know if we try to use our cell phones as we go up an elevator. So there we really need in-building systems, distributed antenna systems or pico cells that will light up the public safety spectrum, you know, not just the commercial spectrum but the public safety spectrum.

So that's a continued push on the building codes and other requirements to make sure on a going forward basis commercial buildings of reasonable size will have indoor systems. And then finally, there will be times where you don't have a cell system where you need it, okay, either because a natural disaster, a tornado's come through, a hurricane, or because the disaster's out in the wilderness area, a train's gone off, you know, the tracks with a chemical spill.

So let's have a fleet of deployables. And again, the good thing in a modern LTE architecture is the deployables are going to be much less expensive, much lighter. Also, particularly in remote America, people get out to the emergencies by vehicles. Turn those vehicles into relay systems. So that's our total plan. The plan focuses -- could we have that, back one please, yeah. The CAPEX funding focuses on the bottom and the top of the pyramid, the middle parts will be addressed through requirements and also

through the operators being able to achieve a return of fair and reasonable rate, and we'll go into the details of that plan in more detail.

Now we're ready for the second chart. Just going to highlight the cost today, we've had details meetings with public safety going through the cost model in detail, and we've verified that with a lot of operators and equipment manufacturers, so we're pretty confident that our costs are good numbers that we've put into the request to Congress. $6.5 billion CAPEX, and an ongoing OPEX that will grow to about $1.2, $1.3 billion in year 10.

On the CAPEX, we again, to be pragmatic, we said, okay, to serve 95 percent of Americans, okay, 95 percent of the POPs in America will have LTE by commercial forces within the next five years, based on announcements of vendors, what's going to happen in the commercial market. In fact, the announcements are actually more ambitious than that, but we said they'll miss their dates by a year or two but not by more than that.

So 95 percent of America will be served by LTE, that means the cell site architecture, the back haul architecture and all will be driven out there by commercial market forces, let's capitalize on that.

We estimated that it takes a little over 40,000, 41,000 cell sites will be needed to serve that commercial architecture and light up the cells that you have to light up for public safety. Again, we think that's conservative, you could probably do it more like 35,000 but we said, let's do it with 41,000.

A little under $100,000 per cell site, $95,000, multiply that out, so that's $4 billion to light up the commercial, take the commercial assets, allow public safety to partner with whomever they choose through an RFP process, to light up their spectrum. So now with $4 billion furnished, we hope, through the appropriations process from the Federal government, public safety now has their spectrum lit up nationwide.

We also said we'd like those sites hardened, structurally hardened, battery backup, et cetera. So we put in $1.5 billion for that. Then we said, we still have to serve rural America -- oh, I should say, and that's to serve handhelds, because that's what that is going to be built out to. In fact public safety will have better service than the average consumer you or I because they'll have handhelds but presumably they don't care as much about form factor and coolness, better batteries and a little, you know,

antenna on top, they're going to have better performance and better coverage than the consumer if we get the right device ecosystem, and we'll talk about that later.

And then, we've got to serve rural America. Okay, rural America we said it's not pragmatic to build out the handhelds to cover vast amounts of rural America, but we do want to get from 95 to 99 percent of the population, so we said we'll build a network for vehicular coverage. So you're now hitting, you know, antennas on vehicles high gain devices, we think you can do that with a little over 3,000 towers -- again we estimate that in many different ways.

And so we'll build out that, put in $800 million to build out in rural America because those sites, we won't have an LTE infrastructure, so we may have to use 2G sites, we may have to use LMR sites from public safety. We thought, three quarters of the cases we can find a site but we've got to build a whole 4G infrastructure on that site, quarter of the cases we may not even have a site out there, so there we put in money to build new towers.

So that $800 million gets you the buildout to 99 percent of America. The program did not include funding for the devices, but by using LTE

infrastructure and the components and guts of commercial devices, we think the device costs can be driven down from several thousand dollars today to the several hundreds of dollars, so that's a tremendous improvement in the budgets for public safety.

OPEX -- and then, oh, I'm sorry, we also put in $200 million for this fleet of deployables and for equipping vehicles in rural areas as relay stations. OPEX, our model is there would be a fee on broadband consumers' bills, the same way we pay a fee for 911 today, not very large, you know, less than a dollar per month, and that would fund the ongoing OPEX growing to $1.2 or 3 billion in year 10.

That would allow public safety to pay whoever their commercial partners are, operators or systems integrators, to operate that RAN infrastructure that's up on the tower, okay, the antennas and electronic processing and all that takes care of their spectrum, pay to transport their bandwidth, their bits or packets, back to the public safety agencies through a standard IP network in a secure private way the way it's done for the military and other mission critical enterprises.

Additional costs were thrown in for rural America because you always have additional costs in

that environment. We did say when they have to use the commercial network for priority access, as the Chairman said in his speech, that would be through commercial agreements but at a most favorable nation type of approach. So that's our basic approach to cost. I'll turn it over to John for technical details. Thank you.

MR. PEHA: So that was two slides. I think I'll be moving a little faster through the other eleven, but you have the slides, I believe, if you want to see the details. So I think we have a very both effective and cost effective strategy here with a lot of elements to it that sort of build on each other. Just to run through at a high level what some of those elements are and then I'll drill down a little on a few of them.

We envision authorized network operators deploying and operating a broadband network designed specifically for public safety and public safety's unique needs in 10 MHZ of spectrum. In some regions we expect this to be an incentive based partnership with a commercial entity, and I'll talk more about that in a minute. Others may already have their own infrastructure which they can use as well.

Another important element of this is, as

Stagg has already commented on, is public safety's ability to use commercial networks in their area by roaming and on a priority basis. Again I'll also comment more about that. Another very important element, as Jamie Barnett has discussed, is funding for network construction, operation, and evolution. We have grants for capital expenditures and the broadband fee for operational.

This makes a nationwide buildout of infrastructure possible, including rural America, and also where infrastructure exists it can help harden it to meet public safety requirements. Fourth important element, requirements that will lead to the creation of devices that serve public safety and operate in public safety spectrum. And finally, to make sure that this is interoperable that there are standards across regions, an Emergency Response Interoperability Center.

So we envision this as a network that will support diverse services and divers application, data and voice services over an IP based transport system from the beginning, forming what is initially perhaps a more reliable version of sort of cutting edge commercial offerings, and then evolving to support mission critical voice and video and data as well.

And we see at least 256 kilobits per second per device even at cell edge to support things like video.

So priority is a piece of this. Priority, or rather, priority access and roaming, public safety users would be able to roam onto up to 70 MHZ of spectrum that is licensed to commercial systems. This obviously gives them access to a great deal more capacity. Maybe less obvious but it is also important for dependability. If the hurricane takes out the public safety cell tower which is closest to you, hopefully some other tower is still functioning that you can use. And similarly, having multiple networks improves coverage, and operators will recover costs at some favorable commercial rates.

We think the technology, you know, emerging technology supports very flexible mechanisms that can be configured to meet any public safety need. You can approach this from one of two ways or both ways. This is an IP based network, not a circuit switch network, which means that network operators have the ability to manage traffic in ways that protect important public safety traffic and ensure that it gets the data rates and quality of service that it needs.

Also LTE has mechanisms in the standard that use priority in determining which sessions are

established on the wireless portion of the system and which are maintained. And putting these together, we believe much can be done and the FCC will work with public safety and commercial wireless services and vendors to determine the precise needs and figure out how systems can be configured to meet them.

So Stagg talked already a lot about the cost model. You know, we had do develop a pretty detailed cost model to try and figure out how much money would be needed, and along the way I think developed a strategy which while it isn't entirely mandated is an effective blueprint for those who choose to follow it. Part of that strategy as you've already heard is to separate serving the first 95 percent where there is already a pretty good existing foot print, and the last 5 percent.

Within the first 95 percent we believe you can overlay the commercial LTE network. There is already, you know, cellular infrastructure out there that reaches 290 million Americans. Public safety can use these, these same towers, to get the coverage and signal reliability they need for a much smaller number of users. And we estimate 41,000 towers should be plenty to do that. And I'll talk a little bit more about the devices, but that's also assuming devices

that are essentially what commercial users are already using, or ruggedized versions of those.

For the remaining 5 percent we see something a little bit different, where vehicles play a larger role. So public safety again will use and harden LMR, whatever towers exist, but we also know that there will be some additional towers that may be needed, and that was figured in the cost. And to reduce the number of these towers we also imagine externally mounted antennas and perhaps repeaters placed in cars, fire trucks, police cars, that can help you get in building coverage or in the area of the incident.

So we also built into this cost model that the system would be designed to meet public safety standards, which may be more stringent, and relied on NPSTC and PSST stated requirements for things like path loss to make sure that you had the coverage you need, perhaps better than some commercial cellulars will provide, or cellular operators. And that's at least the 95 percent. For the highly rural areas, as I said, we assume the vehicular systems play a useful role as well.

And the cost model assumes these commercial technologies for mobile handsets, or variations of them. That in some ways is a conservative assumption

in that if you allow your devices to have external antennas or transmit at a higher power you could do even better, you can get better coverage, better data rates. But we made the conservative assumption, and we think the value of that can be seen by thinking about the device ecosystem. That is, there's a great opportunity to leverage LTE to get commercial economies of scale as long as you can reuse components.

And you see down here a chart with different columns for different pieces of a mobile device. The portions that would be most expensive to customize, like the RF chipset and the baseband chipset, is if you can reuse those by having similar requirements, you get to take advantage of those economies of scale and we believe you can have costs that are close to what an unsubsidized commercial device might have.

So also built into the cost model is this idea of incentive based partnerships which we think have many advantages, increased redundancy and reliability, improved capacity, reduced cost, even improved commercial infrastructure because if you put them together you improve one you can improve the other, transition path to increase spectral and operational efficiency, and this ability to use

commercial technology.

And in thinking about this, we thought of a wide range of sharing possibilities, from public safety having its own system on the left, a dedicated network, to full sharing on the right, and we came to the conclusion that a very cost effective approach was actually something in the middle, in the red box, where public safety has its own dedicated radio access network and can control that and configure that to meet its needs, but it can take advantage of commercial towers and commercial back haul wherever it can find them, and that met for a nice compromise.

And I love the figure with the antennas but I think we're behind schedule, so I'll skip it. Stagg has already talked about deployables, we imagine sort of two flavors of them, one is a cell site you can move to where it's needed, whether that's an area where the hurricane has taken out your infrastructure or you just need to supplement, and the other is these vehicular systems where particularly in highly rural areas you can move capabilities where you need them.

So summarize, I think we have a plan that ensures that broadband wireless communications for public safety will be fully interoperable across all geographies and all jurisdictions, ensures nationwide

coverage. Part of ensuring nationwide coverage is providing funding for the construction, operation, and evolution of this network. We have provide for reserve capacity and redundancy and reliability through roaming and priority access to commercial networks. And ensures that the public safety will have handsets available at reasonable consumer electronic prices. Thank you.

MR. KNAPP: Thanks, John and Stagg. Let me introduce our distinguished panelists this morning, and they're seated at the table in the right order of presentation, which happens very rarely. Allan Sadowski is the Information Technology Manager at the North Carolina State Highway Patrol. Robert LeGrande is former Chief Technology Officer of the District of Columbia Government and the President and Chief Executive Officer of LeGrande Technical and Social Services. Patrick Ringqvist is Vice President Wireless Network Solutions at Ericsson. Roger Quayle is the Chief Technology Officer and cofounder of IP Wireless.

Mark McDiarmid is the Director of RF/RAN Systems Engineering at T-Mobile. And Dale Hatfield is the Executive Director of the Silicon Flatiron Center at the University of Colorado at Boulder. And the

only panelist who has not been introduced is Walter Johnston who is sitting down there at the end who is the Chief of EMC Analysis Division in the Office of Engineering and Technology. You've already met Stagg and John. And so, Allan, if you could start with your presentation, and I am going to hold each of the presentations to ten minutes so that we can pack a lot of information in quickly, and the clock has started. Thank you.

MR. SADOWSKI: Thank you. I have to open mine up with, it's one perspective, I don't represent all public safety but I'll try to do my best. And I do have a standard disclosure that I have to do because it would take too long. I have to hit these I guess. And so it just simply says, I may be wrong and my organization will back me up until I am wrong.

(Laughter.)

MR. SADOWSKI: Okay, let it be clear that because I'm a public safety representative my focus is the mission of public safety. IT and communications is not the primary mission of public safety, it is taking care of our citizens. We respond to incidents and events in rural areas, the tribal areas, wildernesses, out there on the water, and in parks. And for my folks, that's critical that we can support

them in those areas.

Even with no communications at all, public safety is going to respond, it's going to execute the mission. But I hope that the great effort that the Admiral's staff has done, the Admiral and his staff, will help these public safety first responders do their job that much better. It's been hammered here and I'll hammer it again, coverage. Not just cities but also those rural park, tribal, maritime, wilderness areas. And affordable, a lot of these agencies are very small.

I have an instance in my state where the officers pay for their own data access out of their own pocket. That's just not acceptable. And we need it now. Existing systems that are out there that some of us have are very low data rate. Give you an example, the system I live this right now in North Carolina, it's 10 kilobits per officer in a county. All the officers share that same 10 kilobits.

We need the throughput, and I won't bang that too hard, the other gentleman here will certainly hit that, but I like what I hear. Interoperability, we must have it, and we need to have the coverage beyond geopolitical boundaries. The day of this police chief saying, I don't like the sheriff, that's

fortunately gone away to a large extent, because incidents and events do cross to boundaries.

IP and application rate control, everybody here agrees to that, and it needs to be secure. I like what I've seen for reliability, I won't go into it any more, I mean other folks will, but public safety needs the most reliable system it can get. And although this won't be as well received, based on what the mission that we're executing today, data and pictures are more important than voice and video for this system.

Not to say that voice and video isn't something we want, we do, but I'm very guarded about how much data and where I can get it out in rural areas. So I've got voice systems that we are going to keep, we are going to fall back on, so the issues of being able to get some data and some pictures certainly means a lot to my officers and the other first responders that I work with. And I like what I hear about coverage in rural areas so I won't beat on that drum too much more.

I think these are motherhood and apple pie, it means that the responders with the data capabilities will spend more time in the field instead of in offices which are the places that they have data

in many cases today. They will be able to communicate across all jurisdictions and levels, execute the mission faster, make better decisions, and have more reliable and secure communications. So again, I'm going to beat the clock by a good amount. I want to just say thank you to the FCC and to the Public Safety and Homeland Security Bureau, the Admiral and his staff, for this opportunity.

And I will say in the two hours of this group's meeting, public safety will have answered almost 50,000 911 calls. That's not the total number of calls, that's 911 calls. The mission is what it's all about, and I hope, you know, that we will stay focused on that mission, that secure interoperable mobile wireless broadband would help public safety respond to those calls, and that ultimately that data is increasingly becoming of interest, so public safety will benefit with the increased attention paid to interoperable wireless broadband data communications, not just voice. Thank you.

MR. KNAPP: Thank you, Allan. We're going to hold the questions until after all of the presentations. Robert?

MR. LEGRANDE: Thank you. So do I get his five minutes? I just want to know.

MR. KNAPP: Only if he yields.

(Laughter.)

MR. LEGRANDE: Okay. We're partners, he yielded. Okay, so first before I begin I just wanted to thank Jamie, Jennifer, Stagg, and I'm looking over here, John -- you see the ADD, I'm going in both directions here. Really, guys, you've done a great job with this plan, and I can say that sincerely. And I also want to compliment you on the meeting we had last Tuesday, it was spirited but it was necessary, and I'll say it was one of the best FCC meetings I've ever had, because you gave us an opportunity to really dig into you -- no, I'm sorry -- just dig into your plan, and I think that that was important for us to be able to do that.

The comments today I represent are going to be representing APCO's position, and I thank APCO for allowing me to give that. So let's move to the next slide. Oh, I just shut this thing off, can we stop? Okay, I've done something to this and I don't know what I've done. Okay, good. All right, thank you. First I just want to talk about the vision. Everyone shares the vision, which is a national interoperable broadband network that involves seamlessly interoperable networks throughout the country.

I've taken that vision and I've broken it down into various color coding to help present the presentation today, and I want to draw your attention to the amount of green on this chart. On education, training, standards, the goal, funding, research and development, operational procedures and exercises, and the ruggedized devices, as I'll talk about in a second, that plan and the plan that you guys are promoting is in the right direction, and we're very happy with that, and we're going to partner with you to the extent that we can to help you promote those things.

Now, obviously, you know, no plan ever is perfect, and I wish it were, quite frankly I'd love to see all of this was green, but there are some areas of concern which I'm going to highlight today as well. Let's move to the second chart. So first the good news, all the great news I should say. Leverage networks. You know, there's a lot of emphasis, Stagg, and I want to talk about this a little bit later, on commercial infrastructure.

Now, public safety has a lot of existing infrastructure, millions of dollars, particularly after 9/11, has been spent in infrastructure that they can take advantage of that was already hardened. And

so I'd like to talk a little bit about that later on because some of what I'm hearing right now puts a lot of emphasis on the commercial carriers, which it should be, but I think we should also make sure we put the right emphasis on the existing state and local jurisdictions' infrastructure. But the plan's right on, it gives the flexibility to do that and we think that's right.

Funding. Well, let's just start and stop here. I mean the focus that you guys have put on funding is dead on, and thank you for that. And I think I can speak for APCO to say that we wholeheartedly support that effort. We're going to support the effort whether it's here, whether it's on the Hill or wherever we have to go, because we all know that none of this will work without funding. So that's a very important thing.

Now, obviously you've put a lot of emphasis on technical and operational standards. Those are very important. The technical standards, certainly we embrace LTE, and we would like to promote that and move that forward to an official standard, but we also need to get the operational standard. Keep in mind, gentlemen, it's a new world order, voice video and data, never done before, never be done over a single

network, and we need to have corresponding operational procedures that go along with that. But your emphasis throughout the plan on that is great.

Voice communications, as I just mentioned voice, video, and data coming together, it's very important that we have a migration path as a part of the plan that shows how we get from voice, we just don't jump from voice to broadband but we migrate to broadband. Ubiquitous national public safety network, while obviously a network of networks with operational and technical standards that are shared across will get us there, with the investment.

Ruggedized voice, video, and data devices, truer words could not be spoken, I gave a lot of emphasis on that when we were out in Vegas last week because that's a very important part of achieving this goal is making sure that we have the right devices to do it. So on the issue of spectrum, well, let's just start with we know that the spectrum fight is on Capitol Hill. So let's just, you know, I'm not going to go into a whole lot of what, when, and why.

I've obviously had to represent here why public safety's position continues to be that we need the spectrum, you know, and we've outlined that in a website, it's d-block.net, and it goes into a lot of

detail on why we feel we need the spectrum. So but we recognize that you guys' hands are tied to legislation and we're actively working with folks on the Hill to deal with that. Now, we hope to have hearings and we hope to continue to dialogue with you guys in the process. But as far as the spectrum, it's red because it's something that we have to deal with on the Hill.

Roaming, priority, and preemption, we had a lot of discussions about this in Vegas. The short answer is that we're a little bit concerned that the spectrum calculations place too heavy of a dependence on our ability to roam on the commercial network. Keep in mind that we've never done this before. And because we've never done it before, we're going to move to a public safety setting where we have lives in our hands.

So we really want to be careful with that, but again this yellow can move to green if we work together to make sure that we have solid roaming and priority model setup, and that's something that I'm here to let you know based on what I've been directed to tell you we're here to work with you to help you with that, but they have to be incident based models, they can't be application based models, okay?

Next page is early deployments. This can

quickly move, you know, over to aqua, based on what Jamie said earlier, to the extent that we can get these early deployments out. Short answer is I've done two early deployments, and we learned a lot from those. And it's hard, certainly there's risk, but I'll tell you the reward is great. So as soon as we can get to these early deployments you'll inspire industry, you inspire device manufacturers, you inspire use, you actually improve your operations procedures and requirements. And oh by the way, because this is an evolutionary process, this is where we need to start that evolutionary process today, not tomorrow, today. So to the extent that we can move that forward, it's great.

Now, on the issue of governance, you know, nobody can really argue with what you said with ERIC, they're all the right words, there's no question about it. It's just I think the leaders want to meet ERIC. You know, I know, Jennifer, you were going to introduce us to your husband, but we want to meet ERIC, you know, and know that ERIC has the right people quite frankly and the right positions to make sure that everything you said you want to do with ERIC can be done, that's as simple as that. So once we get past that, I'm sure we can move that over to green.

Now, on full multimedia applications, you know, the short answer is, a lot of applications, a lot of the things I've heard so far, even in the New York report, are kind of present day thinking. Well, think about it, we're making a spectrum decision allocation decision that might last ten years, so we have to choose solutions that are beyond our current thinking. So much of this is focused on what we do today and what the carriers allow us, quite frankly, to do today.

But take for example, as soon as these firefighters are able to have helmet cams and those guys can go in there with helmet cams and send back, can both download and upload video from inside a building, they're going to want to do that. When I was putting in the first 700 MHZ network in 2004, the first thing the bomb squad said to me is, we want to use this for our robot, because we don't like standing 100 feet from our robot driving it around, we'd like to be on the other side of town just like you guys. Well, you know.

You know, and then when I talk about drones and things like that, I mean when these guys get their hands on these tools, we should make sure that they have a reliable network that'll be able to -- make

sure that we can meet that demand in the future. I'm not going to go into this chart, it's kind of self explanatory, it's the architecture chart, we've talked about in great level of detail, but it's something that we share the vision of.

The next chart here is in a cost model. Keep in mind as you guys have been talking about the basis of this, you know, we actually in state and local jurisdictions have to really really justify investments, especially today. So going through this very simple cost model will drive whether we use a commercial network or will drive to use our own network. And the thing about it is the basis of this is to not assume that one size fits all. And that the plan already provides for flexibility but this cost model will drive a lot of what you said earlier, but I really have no objections the way you've done the budgetary number quite frankly, so this is just to help with that.

Now, this process chart I'll end on very quickly. There's a lot of work that I tell you from personal experience that needs to be done before you launch a network, and so this was put in here, APCO asked me to put together some training, I did that for them, to try to prepare the APCO membership on getting

ready for broadband. That was done actually a year ago, and it really was set up to give you a sense of the types of things that you need to do in order to make the decision of which way to go in the cost model I just showed.

So I've provided this before and hopefully it'll be beneficial to you. Now, in the last 40 seconds I want to reiterate a couple of things. The plan I workable, we really do believe it's a workable plan, it shows a lot of progress, we're excited about it. Obviously I've identified some things that need to be worked on. We want to partner with you on those things, and especially we want to partner with you on funding, because as the President stated, I am so happy he has said that, void of funding we will not be able to properly serve our citizens. So thank you for your time, and it's yours.

MR. KNAPP: Thank you, Robert. Patrick?

MR. RINGQVIST: Thank you very much. So I am very pleased to be here today and hear, see the focus of the mobile broadband technology for public safety. So I'm representing Ericsson here, and in our mind LTE is the choice for the next generation mobile broadband technology, not just for commercial operators but also for public safety. So I will just

today talk a little bit about some of the key features of LTE that we see and how it relates to public safety.

So let me first start off with reiterating that LTE is a global standard, as you all know. It is adopted by mobile operators worldwide, it is being launched this year worldwide, and this creates a global economy of scale that attracts numerous device developers, application developers, and service developers. And therefore we have a very rich ecosystem of developers for commercial operators, and this is something that public safety also can tap into and share by adopting LTE.

LTE is a global standard, and as a standards based technology it supports interoperability and ensures interoperability. Interoperability is built in from ground up in LTE by adopting open standards. And we know interoperability is one of the key features that public safety requires, so by adopting LTE you will have that. An important aspect of interoperability is roaming, both from a national point of view but also from a global point of view.

And as we can see in the National Broadband Plan, roaming is a key feature to help public safety, not just in coverage but also with capacity. LTE is a

true IP based mobile broadband technology. It supports high broadband speeds with wide coverage. The standards is designed today to support up to 150 megabits per second peak speeds, and we have seen those in trials already today. It uses a very spectral efficient technology and also a very power efficient range of technology, and this enable handheld and other form factors or devices that are desirable by public safety.

LTE has a very low latency or delay on the radio interface. This is a key feature to enable real time services. So it's not just for data services, but also for video communication, voice communication, and other real time multimedia services. And to provide the multimedia services LTE is complemented by IMS, the IP multimedia subsystem that is defined by 3G PP. We see IMS as an important part of any next generation mobile broadband network, and we would like to continue the dialogue with public safety on how to deploy IMS to support these type of services.

LTE is an always-on technology. What we mean by this is that the user is automatically authenticated and connected to the network and to the services that they so want to use. And so when they invoke service there is no connection delay because

you're already connected. All of these and many other features is what makes LTE the preferred choice for mobile broadband technology and also the right choice for public safety.

The network that is built using LTE technology can meet the requirements of public safety as they for example are expressed by the NPSTC Broadband Task Force group that delivered their report last year. We believe that an LTE based public network can provide a wide area coverage and with the speeds meeting the needs of public safety. Using the broadband spectrum allocation 5 plus 5 MHZ, you can build a network that can support peak speeds in excess of 30 megabit per second with an average throughput of 7 to 8 megabits per second in the cell site, and this certainly meets the needs of public safety in our minds.

Now, evolution doesn't stop here though. As any standards based technology, evolution continues. So what I'm talking about now is the first general LTE that is being deployed this year. Already now there is work going on in standards body, 3G PP in particular that is the standards body for LTE, on advancements in how to improve the performance of LTE, and many of those improvements are of interest also

for public safety.

One such example is the relay. A relay is a unit that you can place in an area where you have poor coverage, and it improves coverage in that area by relaying the signal from the broader cell into that area. This is a little bit different than the normal repeater because it is coordinated with the macronetwork so you can have a better coordination of handovers and other things.

Now the improvement that's also being worked on is something called coordinated multipoint reception. What this is, is a technology that is intended to improve performance at cell edge. It does this by avoiding some of the interference limitations that you have at the cell edge. So both of these examples, and many others, are now being evaluated and explored in the standards bodies, and they're targeted for being standardized by the end of next year and being available commercially 2012.

Lastly, I want to say a few words about priority services. We heard a lot here today about that priority and preemption are important for public safety, and we have known that for quite some time. LTE has a rich set of quality of service capabilities, and these capabilities, they enable LTE to meet the

needs of public safety in this regard, enabling public safety to differentiate between different services and different users, thereby establishing the hierarchy of admirals before generals et cetera.

What happens now if a public safety user roams to a commercial network? Well, in the 2G networks of today, we have the wireless priority service WPS for voice networks, so that is of course available for the traditional 2G networks. Activity is now ongoing to take that same type of principles and standardize it on an LTE network. This is ongoing in 3G PP as well as the next generation Getz forum here in U.S., and they are coordinated.

So through these new standards, the same type of service concepts can be transformed and moved into a packet network, and thereby extend priority access from voice to also include data sessions and multimedia services. And unlike today's WPS where you have to dial a long access code to get access to the voice service, you can also have other capabilities on how you set the priorities. They can for example be set up so that you're authorized for the service right when you connect to the network for a particular service. In this way, the WPS service can be much more seamless for the user.

Since LTE is also a package service, the way the priority is done is different than in the traditional circuits switched 2G networks. So you apply the prioritization on each packet, not only at the establishing of connection, and thereby you can in real time have a much better flexibility in how you handle priority. So in conclusion, we believe that LTE is the next generation mobile broadband technology, and it is launched right now by operators worldwide. We also think that it is the right choice for public safety and that public safety by deploying LTE will have a rich set of multimedia and data services with a rich set of devices available to them. Thank you very much.

MR. KNAPP: Thank you, Patrick. And for the record, all of our speakers have done a fabulous job of staying under ten minutes, thank you all for that, so let's just keep it going. Roger, you're up next.

MR. QUAYLE: Thank you. There has been a lot of discussion about LTE devices for the 700 MHZ band covering the public safety and D block, which is band class 14 and 3G PP. So the Commission has asked me to speak about the 3G PP band classes and the support of the various different allocations in the 700 MHZ band, and also generally about the public

safety device requirements. And also, Stagg and others have mentioned the various options that exist for improving coverage for public safety in rural areas, so I'll be speaking about that as well.

If we look at LTE, as Patrick said, it is truly an international standard. That of course means that the technology needs to be standardized to cover a wide range of bands in countries internationally, and ideally a user device should be able to support as many of these bands as possible to facilitate very wide international roaming, and we are starting to see that now on 3G phones, which can now roam between the networks in the U.S. and Europe and also now more recently into countries like Japan which have traditionally had different frequency bands.

The issue this creates for the device manufacturers, if you look at the chart you'll see that there are in total about 30 or more different bands that a device has to support for international roaming. You'll see a very wide range of FDD, or frequency division duplex, bands for LTE, both FDD and TDD. And then also a device needs to support up to seven or even eight, nine, or ten UMTS and GSM edge bands for international roaming. So it's not so much a technical issue, it really comes down to a practical

and commercial issue as to how many bands a manufacturer wants to put into a user device.

So if we look at the 700 MHZ band, and you'll see band 14 at the top, which is the combination of the public safety allocation and the D block, you'll see that the current mainstream device vendors are supporting band 17 and band 13 because they have to date made their choice to limit the number of bands they're covering, not so much because of just 700 MHZ but because of all the other bands that they need to cover.

So there is an issue currently with the devices from mainstream vendors covering the public safety allocation. IP Wireless has a device, a really 7 3G PP device that's FCC approved that does cover the whole band, and I'll describe on the next slide how we achieve that. The LTE standards define user devices as being able to operate in either full duplex FDD mode or half duplex FDD mode. The main difference in performance is the peak rate that a user can sustain.

However, in a loaded network we're more concerned about the average throughput that a user sees and not the peak, and in that respect there's very little difference between full duplex FDD and half duplex FDD. So one option a device manufacturer

has is to use half duplex FDD, in which case there's really no issue in covering the entire 700 MHZ band in a device.

For full duplex FDD, separate duplex filters are required for each of the bands. So if we look at the lower part of the band, band 14 and band 17, it is possible to have a filter that covers band 12, which then incorporates band 17. We believe the reason that vendors have not done this so far is to protect against adjacent channel blocking from media flow which is in the middle of the lower band, and also UHF television which is down in the 600 MHZ region immediately below the 700 MHZ band.

Then in the upper band, it would be technically possible to have a duplex filter that covers band 13 and band 14. However, the issue is that if you look at the upper end of the lower part of band 14 and the bottom end of the upper part of band 13, there's a very small duplex gap, which makes it more challenging for the filter developer. It's not to say it's not impossible, it's really a tradeoff between the overall size and cost of the filter.

So band 14, as I said, is not covered currently by the commercial UE vendors, and as I said it's really not a technical issue. With full duplex

FDD UEs, they do have to make tradeoffs and choose a subset of the bands that they're going to support. However, while we're all disappointed that public safety may not get the D block, one of the sort of compensating benefits if the D block becomes a commercial band is that it will ensure that there are commercial devices that cover band 14, which then solves the band coverage issue for public safety mobile broadband.

Looking at devices, one of the benefits of LTE that Patrick has touched on is the economies of scale of public safety being able to take advantage of the huge volume ecosystem for LTE which is going to go into tens of millions and potentially billions of devices ultimately when it gets embedded in the 3G PP operator ecosystem. That is clearly true for the components such as the base band chipsets and the RF chipsets, and it's true for standard commercial user devices, like for example a PCI express minicard which is embedded in a variety of devices, or a USB stick.

However, what we see from our experience in public safety, for example with the NYS1 network in New York, is that public safety do have unique device requirements. One thing that's often overlooked is the temperature range of the device. You can have a

UE and a router in the trunk of a police car that on the east coast or the northeast might be in the precinct parking lot overnight in very negative temperatures, and then it might be in Nevada in the peak of summer. That device has to stand a much wider temperature range than commercial devices.

In terms of form factor, there are special devices required such as rugged routers, LTE UEs embedded in rugged tablet PCs, rugged PDAs, and so on. Commercial smartphones for the public safety 700 MHZ band such as the iPhone and Android, this is really dependent on the commercial operators supporting band 14, because these volume handsets require large volume even to produce a variant for a particular frequency band.

So I know I'm short of time. Moving on to rural coverage with LTE. The commercial networks in rural areas are typically designed for in-car coverage, for example a smartphone in a vehicle. For public safety, there's a major coverage increase that can be had simply by going to vehicle rooftop antennas and getting a combination of removing the vehicle penetration loss and getting an increase in antenna gain.

So if we look at the following chart, this

is just indicative for a rural area, and what you'll see is the first circle, the red circle, is a smartphone inside a vehicle. We then go to a smartphone outdoors, and then we go to a vehicle rooftop antenna, you can see how coverage progressively increases, and then ultimately to an option which doesn't yet exist in 3G PP power classes, to go to a 1 watt, or 30 DBM, UE.

Likewise, if you look at a handheld device, a typical smartphone has internal antennas which 700 MHZ will have unity, or zero gain, at best. Simply by going to a rubber ducky style antenna on a rugged public safety handheld device is going to give an increase in coverage. So I'm just about at my time now so we'll finish at that.

MR. KNAPP: Thank you, Roger. Mark?

MR. MCDIARMID: Very good. Thank you very much, Juli. I just want to take a couple moments to thank the FCC for the opportunity to address the audience today. My name's Mark McDiarmid representing T-Mobile USA. And what I wanted to do today was walk the audience through a couple of slides relating to some of the aspects of let's say commercial asset sharing, and how that works and how it has worked in the past.

First, I want to say a couple of things about the idea of sharing infrastructure. Within the commercial operator community it's something that we've done before, and certainly at T-Mobile US we've done it with some of our competitors in the U.S., both on the west coast and in the northeast, where we have shared access networks successfully over major metropolitan areas, but yet retained control over the switching infrastructure and the billing and rating plans that make us ultimately very competitive, and that arrangement had been in place for many years and what very successful for both the parties.

So the concept of infrastructure sharing is not new, and within the commercial carrier community is practiced and well understood, certainly in the domain of both 2G and 3G as well. And the question would be, how would that translate to a possible public safety commercial operator arrangement or collaboration to share infrastructure? And there are really sort of four key elements to that that I want to work through.

And let me start by addressing the core networks, and in this LTE network architecture, we would assume that the core network would be implemented using the IP multimedia subsystem, or IMS,

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.

Thank you.

MR. KNAPP: Bob?

MR. GERSE: Hi. Bob Gerse with APCO. I know this is a technical panel, and let's make an assumption that all the sharing, priority access capabilities that you talked about are there and to address Robert's point are proven to be operational. I guess a concern that still is there is, if I'm a carrier, even though I may get compensated on some sort of a best customer basis, why would I want a situation where I have to on a moment's notice give up access, give up capacity on my network, for public safety?

And assume also that if you give these toys, these devices to public safety, they will use them and they will use them a lot, and it's not going to just be a 9/11 situation where capacity gets eaten up, it's going to be every time there is a significant fire, every time there is a snow storm in D.C., every time there's some major event, there is going to be a tremendous spectrum demand, and let's assume you only have ten, that's going to go beyond that. So I guess it's more of a regulatory question, but how do we make sure that the access that's technically available is in fact available?

MR. KNAPP: Anybody want to take that one? Stagg?

MR. NEWMAN: I would address that in a couple ways. Obviously we have to get out there and get experience with what demand will really be. I think we start off the next, the first few years, in a good situation in the sense that if you look at the commercial operators today, say Verizon, they've got close to 100 million customers I think after the merger, they're over 90 million. And they have typically 80 to 100 MHZ per market. So they've got about 1 Hz per user of capacity.

Public safety starts out with 3 million users eligible but effectively probably more like 1 million users, because the volunteer fire departments, with 10 MHZ. So they're starting out at 10 Hz per user, so a lot more user on their core network before they go into the priority. Now, they are going to have incidents where it's much more focused in particular sectors, and so we have to develop the business arrangements that go with the technology arrangements.

I mean when the police and fire, you know, are at a scene, we accept we can't use those roads during that moment, right, and you know, the roads get

blocked. So I think we have to work out the business arrangements, and just like commercial operators have to support 911. Now, I don't know the whole history of how that deal was done, actually probably dates back to when there was one Bell system it was a lot easier than dealing with lots of commercial operators.

But I think technically we've got some head room. And the Chairman said in his speech that as we free up more spectrum, public safety will get more of that. So I think we have a path forward, but I think one of the speakers, it might have been Patrick, made a very good point, we've got to get out there, you know, get experience, the FCC has got to use their leverage to make sure public safety needs are met, and come up with a working solution. Dale?

MR. HATFIELD: Well I was just going to add that we talked a moment ago, emphasized a moment ago, about the additional cell sites being able to help solve the coverage problem, but I agree with Bob, there's going to be lots of these applications that are going to keep pushing demand for spectrum. And I think ultimately a lot of that solution has to be in frequency reuse and smaller cell sites. So while we emphasize the coverage aspects of it, I think long term it has to be also aimed at increasing capacity

dramatically.

MR. KNAPP: Thank you. Harlin?

MALE SPEAKER: I'm here speaking on behalf of the Police Chiefs Association and the Public Safety Spectrum Trust, and a couple of things I want to comment on and hopefully draw some response. First of all, we start with almost the end of the panel when Dale talked about the sharing aspect. And we have always assumed that in one way or another there would have to be some shared aspect of all this, in other words there are going to be a lot of times when in maybe not in the major urban areas but in a lot of the country where we won't be needing all of that spectrum, and certainly sharing that makes sense.

It is the fact that right now, if we don't get the D block and have the ability to enter into public partnerships with people to do that sharing, then there needs to be a more sure mechanism as to how we have access to the other spectrum to do that sharing, and that doesn't seem to be, there isn't a clear path for that at the moment, that's something that really concerns us.

And then that leads to the comments that Stagg made and Patrick made about the throughput. So help me a little bit, because for those of us that are

not technically qualified as some of you, Stagg, you say in your slides cell edge, the plan is that we would get hopefully at least 256 kilobits per second at cell edge, okay, and Patrick's talking about with 5 by 5 this is wonderful because we're going to be able to get 30 megabits per second. Now, there's a hell of a gap between 256 kilobits per second and 30 megabits per second, and the question is, I guess to you, Patrick, first is, with your vision of 30 megabits per second, how far does it go when you get to the cell edge? I mean how bad does it get?

MR. RINGQVIST: Yeah, I can address that. So I think the important factor to look at is on an average throughput. So yes, the 30 megabits is peak and it's under ideal conditions, it's very rare that you will get that. The average is what you will get from an every user in the cell distributed with an average would get. That is more relevant and that's more what you design your networks for.

What I stated there is that 7 to 8 megabit per second is what you would get as an average, seven to eight. The cell edge is where you have the worst conditions. And so what Stagg mentioned there was 256 I think it was, and that is consistent with the modeling of LTE that we can achieve a 256 at cell

edge, so that is the worst performance.

MR. KNAPP: John, John wanted to -- yeah, go ahead.

MR. QUAYLE: If I can just add to that, it's easy to think of the cell edge in very simplistic terms as being, you know, very geographically defined, you know, the edge of the circle. But the cell edge in LTE is really defined by the radio conditions that a user is in. And you might have a major incident which is geographically occurring at the cell edge and you've got public safety users all around, say of a very large burning building, each of those users is, they're not all going to be at the cell edge in terms of the radio channel conditions because a lot depends on exactly where they are, whether they're, you know, inside a vehicle and getting vehicle loss which puts them at the cell edge, or if they're shadowed.

So even, you know, distributed across say 50 public safety first responders at the cell edge, only probably a percentage of those, maybe 10, 20 percent, will be at true cell edge radio conditions. So the bottom line is the others will get higher throughput than the bottom line of 256 kilobits.

MR. PEHA: I was going to say, well also some of what we talk about 256 kilobits per second,

we're talking about per device, which is, you know, just like -- and that's an uplink. So, you know, we guarantee each of you a foot and a half by foot and a half to sit on when you all come in here, that doesn't mean that's all we have in the auditorium. But the initial premise also, you talked about unused spectrum, I think Dale is really referring to dynamic use of spectrum.

If you look at how public safety systems tend to use spectrum, and before coming to the FCC I have, you know, over days, weeks, months, and minutes, you find that particularly in western Pennsylvania, you find that, you know, average usage looks very low because utilization for very long periods of time is very low, and then it spikes tremendously. So it's really worrying only about, you know, the spike, and actually 10 MHZ gives you an awful lot to spike into.

As Stagg was pointing out, 10 MHZ with the kind of frequency use we're talking about is very different than 10 MHZ with the old kind of systems. And then as to whether we have other arrangements, I mean that is what the priority roaming we've been discussing is, and I think the technology easily supports that as well.

MR. KNAPP: Allan, did you want to join in?

MR. SADOWSKI: Certainly, because of who I'm working with I'm very sensitive to this, and so something that I'm hoping to hear a little bit more about myself is the overlap between these cell sites, because I need to know that in a stress situation that the people that I support in fact have the options of going to other sites. And I'm hoping that the technologies will support some directivity with the -- mentioned here, so that it gives them the option of transferring to another site and supporting the public. So, but I do see what's happening here, it's really exciting for me knowing where I'm coming from and the people I support today, they have nothing, a lot of them. So this is really exciting to hear this kind of discussion.

MR. LEGRANDE: I have one -- I hate to make you stand there any longer.

MR. KNAPP: Go ahead, no, sure, sure.

MR. LEGRANDE: You know, there still seems to be a focus on what we can do today versus what we're going to be able to do tomorrow. And the thing that kind of really is, well disturbing in a sense, is that we know that the commercial industry, the appetite for wireless data has grown, as my kids would say, it's ridiculous, dad. They will use that word at

any time, trust me, and so I'll just use it here, but it's been exponential, right?

Public safety has been throttled down, we've been held back. There is a pent up demand right now. We're going to take off the top of that, we're going to give them a network, and this is the first thing you're going to see, trust me, I've seen it before, you're going to have use go out of the roof, the first thing they're going to do is have a video setup for everything, there will be inefficient use, I know that.

But the presumption that we have enough and our tools are going to be enough in this fair radical peak that we think is going to be enough based on current application use is not enough. We have to assume that it's going to go in a direction -- these are going to be the new superusers, they're going to use this network more than our kids are using it today, and we need to make that assumption, design for that assumption, and apply that assumption in everything we do, including of course, I hate to say it, last time, spectrum allocation.

With regards to Dale's point that he made earlier of unused inefficient use of the spectrum throughout the country, well, you know, we're going to

have to go through a maturity model to get to efficient use. I don't suggest we just go to efficient use and demand that public safety fit in a box. I think we migrate to an efficient use such to make sure that they have enough when they need it.

Now, we may have ten incidents around the country that results in, you know, an inability for public safety to communicate, well those might be the ten worst incidences that we would ever have to respond to. So I would much rather make sure that they have everything that we can give them now and then throttle them back through technology, through efficiencies, through spectrum sharing and configurations, and mature to that point, not start at that point.

So that's the difference that I see. I definitely agree, I don't want unused inefficient use of spectrum out there, but I also want to make sure that we avoid that situation I just described. And quite frankly I think that, you know, public safety has already said that they're willing to, you know, share their existing spectrum. So, you know, there will be spectrum that will be available. So while, you know, sure we won't be totally efficient with 700, well we'll be freeing up spectrum, and that offset

should hopefully bring us to a place where everyone can be happy.

MR. KNAPP: I'm going to -- okay, make it quick so I can get to the last two questions and then we can wrap up.

MR. RINGQVIST: Just to comment on the rubber duck, I don't want to make a statement on whether 10 MHZ or 20 MHZ is enough, but whatever you have, I think it is important that public safety understands that you need to manage what you have. So a method for managing the bandwidth available, a method for telling what service, which user is important at this point in time, that is very important. And that's more of an operational aspect from a public safety point of view and how public safety will use the mobile broadband network. The technology is there to allow differentiation between services and between users, and it's up to public safety to define how to use that flexibility.

MR. KRESBIN: Hello. Keith Kresbin, AT&T, and first if I may comment, we support the concept of the D block by the way being allocated to public safety, we think that's the right thing to do. Maybe it's worthwhile to think about how an iPhone has impacted data usage and traffic patterns in the United

States, and maybe that gives you some sense of what Mr. LeGrande is thinking about when he talks about pent up applications and data demand.

So with that comment aside, I do have a question. There's been lots of discussion surrounding the contention between public safety users and commercial users for network access. But if we begin with the Commission's understanding that there would be a private radio access network dedicated to public safety built using their 700 MHZ spectrum, doesn't it sort of make that contention a moot fact? I mean if public safety has its own radio access network, the officers in the field, firefighters in the field, can absolutely have access, and that can be guaranteed on their own dedicated network. So it sort of sets aside this idea, right, of competition between commercial users and public safety users?

MR. KNAPP: Walter?

MR. JOHNSTON: I think this is a great question to open up I think an important issue I'd like actually the panel to discuss, which is, I know that public safety has expressed concerns to us. We have something called wireless priority service, and it's been around for a number of years, and public safety has had some good experiences, a few, and more

often than not they point to the cases where it's failed. And I'd like some of the panelists to address the priority mechanisms in LTE that would allow, when it's required under policy, public safety access to commercial spectrum in terms of what priority mechanisms are in that would allow them and how that's different from the current 2G technology that's available today.

MR. RINGQVIST: So I mentioned in my opening remarks that there is conversation ongoing in this field on how next generation wireless products and service would work on a network like LTE. So this is a fairly complex topic that I don't think we have time to go into too details. I mentioned that there is work ongoing in the next generation Getz forum, they have a draft specifications that they're working on that is 400 pages long, which I will not go through here. So, sufficient to say there is a lot of work, a lot of energy being spent right now on how this should work in an LTE environment. And the place to be is the Getz forum and 3G PP, and I encourage anybody who's interested to take part in those discussions there.

MR. JOHNSTON: But I just want to make clear, we've seen 2G systems fail in terms of priority

access. Do those same mechanisms exist in LTE?

MR. RINGQVIST: No, the mechanisms are very different in LTE versus in 2G. So some of the key things in 2G is that you have to request a circuit and you have to do special dial codes. All those things will change when you go to a package based systems like LTE. There will be multiple ways you can get access to a priority service. You can do the normal way requesting a end to end session or dial code, or you can do it through an application connection time, or you can do it through in-core through some other mechanism. There are a wide range of capabilities being defined in these standards, as I mentioned.

MR. KNAPP: Let's take one more question. Well, let's to the question and then I think we have to move to wrap up.

MR. MURGON: Hi. Dick Murgon, APCO. There was some discussion here touched briefly about future spectrum for public safety, if the growth should, you know, occur exponentially like we would expect. Has there been any thought or can somebody maybe articulate how that gets integrated into an existing public safety network without having to forklift the technology being bought for this broadband process and being able to incorporate something into whether it's

500 MHZ or 30 gig, how that works?

MR. KNAPP: Well, why don't I take a stab at that one. Of course it's always a concern when we add an additional frequency band about how that's going to integrate with existing equipment, and certainly one of the things we don't want to do is exacerbate the interoperability issues. But I will tell you, as part of the Broadband Plan yesterday and having been here at the Commission and dealing with spectrum allocations a long time, I think it's probably one of the most forward thinking approaches to spectrum management that this agency has ever put forward, including our working with the Federal government, the NTIA, to look across the spectrum not only at the bands that we had put on the table yesterday as specific areas, but in a very deliberate process to look at all of the spectrum for opportunities. And I think there's nothing more important both on the Federal side and for us than ensuring that as part of that process public safety's requirements are taken into account. And if as part of this it looks like it's appropriate and there's a nice fit, I think what we've been saying is that's very much part of the mix. Stagg?

MR. NEWMAN: Let me just say, from a

technology standpoint, you know, I don't think it'll have to be a total forklift in the future. Transitions are always hard, but technology over time is helping us more and more. For example LTE envisions not having to have all the bandwidth contiguous, in other words you could take five here and ten here. Now, that's going to require changes, but there are ways to use what you have and use additional spectrum that may not be at all close.

IP Wireless already talked about some of the improvements so that they can take in far more bandwidth with a single, you know, set of devices than you could in the past. So I think, you know, if we look five, ten years out, a lot of these things, you know, all the way to the future, software to find radios et cetera et cetera, are going to make those transitions better.

You know, the reality is it always takes -- I mean software to find radio and some of these concepts go back ten, fifteen, twenty years, but that's the reality is that's how long it takes to get it to the market. But the good news is over the next ten years we're going to bring to fruition a lot of the research efforts that, you know, were on the table when I was Chief Technologist more than a decade ago.

MR. LEGRANDE: I have one quick comment on that.

MR. KNAPP: Sure.

MR. LEGRANDE: I think that my concern with that is, one of the reasons why we chose LTE as public safety is to try to get in the wake of the carriers, right, and try to stay as closely as possible within their commercial technology platform. When we start diversifying anything, I mean from frequencies to any type of requirement, we have to make an assumption that we're moving out of their wake, costs will increase, and even the question of whether or not the commercial device industry will support us will actually become more difficult. So while I don't doubt, I mean we can always say that technology can do it, technology can do it, but we have a business aspect of our technology which is sometimes prohibitive. So, well, like I said before, you know, would always welcome that as being an alternative, but we still know what the best alternative is.

MR. KNAPP: All right, with that, I promised a robust discussion and that's what we got. And I want to thank all our panelists because I thought we've learned a lot today and it was very constructive and we all share a goal of making sure that public

safety's needs are met. And, Admiral Barnett, if you want to just wrap up the session?

MR. BARNETT: Juli, thank you for your moderation of this robust discussion, and thank each of you for being with us today. And a particular set of thanks to our experts for this. I have a couple comments, but let's applaud them now for their great discussion.

(Applause.)

MR. BARNETT: So just a couple of observations as a benediction here. I think what we heard today from my standpoint was very significant, number one, we heard these experts describe, you know, how this network can work for public safety, very significant. Number two I would say is they also focused on some of the things that we need to address next to make sure that that happens, also very significant.

And then I would point out two things. Although I appreciate all of the expertise here there are two that I'll draw out. Number one, I really appreciate Allan Sadowski focusing on what we really need to focus on is it's the mission, we have to accomplish the mission, we have to enable public safety to accomplish the mission. And I also want to

point out and thank Robert LeGrande, also very significant.

In essence what he did, this is a voice for public safety saying, here is a way forward for us. You know, let's take what we agree on and the good parts of the network and let's build on those including, and I really like his green part up there is, we need to go after the funding to make sure that this network becomes reality. So thanks to each of you and thank you for those particular, those significant aspects, and we appreciate your presence here.

(Whereupon, at 11:37 a.m., the workshop in the above-entitled matter was concluded.)

//

//

//

//

//

//

//

//

//

//

REPORTER'S CERTIFICATE

CASE TITLE: 700 MHZ Workshop

HEARING DATE: March 17, 2010

LOCATION: Washington, D.C.

I hereby certify that the proceedings and evidence are contained fully and accurately on the tapes and notes reported by me at the hearing in the above case before the Federal Communications Commission.

Date: March 17, 2010

Gabriel Gheorghiu
Official Reporter
Heritage Reporting Corporation
Suite 600
1220 L Street, N.W.
Washington, D.C. 20005-4018