UNITED STATES OF AMERICA

FEDERAL COMMUNICATIONS COMMISSION

NATIONAL BROADBAND PLAN WORKSHOP

PUBLIC SAFETY AND HOMELAND SECURITY

Washington, D.C.

Tuesday, August 25, 2009

ANDERSON COURT REPORTING
706 Duke Street, Suite 100
Alexandria, VA 22314
Phone (703) 519-7180 Fax (703) 519-7190

PARTICIPANTS:

Panel 1 - First Responders Using Broadband Technologies to Advance Public Safety

JENNIFER A. MANNER, Moderator
Deputy Bureau Chief Public Safety and Homeland Security Bureau

CHARLES BRENNAN
Deputy Secretary Commonwealth of Pennsylvania's Office of Public Safety Radio Service

STEPHEN CARTER
Vice President of Technology, Qualcomm

PETE EGGIMANN
Chair, Operations Committee National Emergency Number Association

RALPH HALLER
Chair, National Public Safety Telecommunications Council

GLENN KATZ
President and Chief Operating Officer
Spacenet, Inc.

HARLIN McEWEN
Chair, Public Safety Spectrum Trust

BILL SCHRIER
Chief Technology Officer & Director of Information Technology, ANSI-Accredited Standards Definition Organization

REAR ADMIRAL JAMES A. BARNETT, JR. (Ret.)
Chief, Public Safety and Homeland Security Bureau

LAURIE FLAHERTY
Program Analyst, Department of Transportation

PARTICIPANTS (CONT'D):

JEFFERY GOLDTHORP
Chief, Communications Systems Analysis Division
Public Safety and Homeland Security Bureau

CHARLES HOFFMAN
Chief, Disaster Emergency Communications Programs
Federal Emergency Management Association

JOHN LEIBOVITZ
Deputy, Chief Wireless Telecommunications Bureau

KATHRYN MEDLEY
Chief, Satellite Engineering Branch International Bureau

ERIKA OLSEN
Senior Advisor, Public Safety and Homeland Security Bureau

DANIEL PHYTHYON
Chief, Policy, Planning & Analysis Division
Department of Homeland Security

Panel 2 - Homeland Security

WILLIAM LANE, Moderator
Chief Engineer, Public Safety and Homeland Security Bureau

ANDREW L. AFFLERBACH
Chief Executive Officer & Director of Engineering
Columbia Telecommunications Corporation

EMMANUEL HOOPER
Senior Scholar and Researcher
Harvard University

MURAD RAHEEM
Branch Chief, U.S. Department of Health and Human Services

PARTICIPANTS (CONT'D):

MARC SACHS
Executive Director National Security and Cyber Policy Verizon Government Affairs

STEVE SOUDER
Director, Fairfax (Virginia) Department of Public Safety Communication

JEFF COHEN
Senior Legal Advisor, Public Safety and Homeland Security Bureau

CHARLES HOFFMAN
Chief, Disaster Emergency Communications Programs Federal Emergency Management Administration

JON PEHA
Chief Technology Officer, Federal Communications Commission

DANIEL PHYTHYON
Chief, Policy, Planning & Analysis Division Department of Homeland Security

* * * * *

P R O C E E D I N G S

MR. BARNETT: Thank you all so much for being here today to discuss broadband issues and technologies and how those innovations can promote public safety and homeland security.

My name is Jamie Barnett, and I'm the chief of the Public Safety and Homeland Security Bureau here at the Federal Communications Commission. Some of you may already know I spent a little time in the Navy. My first job in the Navy was as a communications officer working with HF, VHF, UHF, and a new innovation back then -- it was a long time ago -- called satellite communications. I learned then how important and critical communications is to getting the job done. And another incarnation -- as an attorney that represented law enforcement and municipalities and local governments, I learned what the people on the front line do and how important communications are to them. From that, I think, I gather that we are on the edge, the cusp, of another great technological innovation

and insertion, and I look forward to discussing that and hearing the discussion with you today.

Eleanor Roosevelt once said, "It is today that we must create the future of world of tomorrow." We are, in fact, creating that world of the future as we discuss and develop and embrace the benefit of broadband technologies. As we move forward moving innovative technologies, broadband will play a large role in how emergency responders communicate with each other and with the public.

Today, we will be discussing some of those important issues regarding the use of broadband technologies in public safety and homeland security and how to ensure that important communications are always available to our emergency response community, and really to all American citizens. That, in essence, is our goal, is to make sure that the benefit of these technologies makes our American public more safe; more secure.

Broadband technologies can benefit

public safety and homeland security in tremendous ways. Really, the tremendous group of people that you see sitting in front of me -- and I assure you this is the only time today that I'll be able to speak above their heads -- they will discuss with you and have great insights into what that world can bring to us. But even I can see the amazing benefits that broadband technology offers right now and being able to get the information that our public safety community needs in a quick and efficient manner. We also know that public safety answering points can utilize broadband technologies to a greater extent, and in numerous ways they can assist public safety agencies in making emergency response more timely and more efficient.

I'd like to take just a moment and let's imagine how that future can be and really what would happen. For example, if firefighters could receive a recent video of a fire scene or perhaps blueprints or where hazardous material is located even as they proceed to the fire scene, how they

could be able to save lives, protect themselves, and protect property. Or consider in a law enforcement scenario if citizens could send videos of a crime scene or an accident or even a suspect or evidence, even as the law enforcement officers proceed to that scene. And in the medical response arena broadband offers potential benefits where they could be able to share medical information as they take a patient or victim to the hospital or maybe even the medical records of that person could precede the person before they get to the hospital.

Now, actually, some of these applications are being inserted right now in various places in the country, but too few, perhaps. And I think one of our goals here today is to make sure that we provide a means to ensure that the entire country gets the benefit of public safety broadband.

Now, some of these benefits -- some of these visions that I just mentioned are some of the main drivers for the goals and the major tasks

facing the Federal Communications Commission right now. As you know, the Broadband Plan was mandated by the American Recovery and Reinvestment Act of 2009. The Act requires that public safety be a major consideration in that. In April, the Commission issued a Notice of Inquiry seeking comment on how to implement the plan. In particular, we included Commission-specific questions on how broadband can be used to enhance public safety and homeland security.

So, in addition to the Notice of Inquiry, the Commission has been holding these types of workshops. I've only been here four weeks, but I understand that this is almost an unprecedented amount of activity.

Jennifer, how many workshops have we got scheduled?

MS. MANNER: Over 23.

MR. BARNETT: Over 20, and that doesn't count the ones that we have coming up on the road in the future, an unprecedented level of activity.

Our hope is that today's workshop will

help develop and aid the Commission in gathering data -- and data is what we need -- data fact-based and data-driven information to help us in this process. We're pleased to have the subject matter experts that you see in front of you here today participating, and their valuable input, I think, will really help us along and structure and develop the public safety portion of the Broadband Plan.

Now, the Broadband Plan is due to be delivered to Congress on February 17, 2009. So we are now under six months in having that deadline and we're working really at a very fast pace. Your presence here today, and those of you who are present with us on the web, really assists us in moving this forward. We're looking forward to your information. We want a free flow of ideas, and we realize that we cannot create an effective plan without your input, your knowledge, and your expertise. It's important to the future of public safety communications that we find the right path and create a plan that works to meet the needs of

the emergency response community as well as the public when they need to reach out to public safety entities during emergencies.

Now, some of the topics that will be covered in today's workshop will include ways in which broadband can improve public safety and homeland security; what broadband policies will promise and promote Next Generation 911; to what degree broadband should support mission-critical voice and public safety data applications; how public safety is utilizing the Internet and web-based applications; how broadband can help large-scale emergency preparedness and response; and cyber security issues. Our hope is that the data that we generate here will create a really good dialogue for the future.

Now, I mentioned our experts in front of me and I'd like to thank them for being here today. For all our FCC participants and the people that have come, the other governmental agencies that are here today, I appreciate your willingness to participate in this workshop. I'd

also like to take an opportunity to thank the people that have worked so hard to put this together: Susan McLean, Susan; Stephanie Caccomo you see up here; Deborah Klein; and many others who have worked so hard, not the least of which is Jennifer Manner, who I'll introduce in just a minute.

Thank you to our Washington audience and also for the couple hundred or more people who are attending today on the web. We appreciate your attendance and participation and your interest in this important endeavor and important workshop.

So, in coming to the Commission as I did a few weeks ago, one of the things that really excited me was the level of expertise that I found here, the dedication of the professionals that work in the Public Safety and Homeland Security Bureau and their excitement about this process and about the work that they do. It's exciting to be with people who like to do what they do. And people who want to come back, too.

So one of those people is Jennifer

Manner, who comes back -- returns now to the Federal Communications Commission as one of the deputy chiefs of the Public Safety and Homeland Security Bureau. She's been one of the people, among others, who have been working very hard to get this workshop going and on the great ideas that we have for the future. At this point, Jennifer, I'd like to turn it over to you.

Thank you so much.

MS. MANNER: Thank you so much. Before we get started I wanted to just walk through the agenda and some of the ground rules just so our panelists are all on the same page, if that's okay with everyone.

So we're going to start off at 9:15 with Panel 1, and then at 10:45 we're going to have some brief comments by Dan Phythyon from the Department of Homeland Security, and then turn the floor over to Charles Hoffman from FEMA for a few brief comments. After that we're going to take approximately a 10-minute break, and I'd request that everyone come back to the room by 11:05 for

our second panel on Homeland Security issues. And then we'll just have some brief closing remarks.

I do want to urge that we need to try to keep this workshop on time because we have another workshop starting 45 minutes after this workshop. So, I appreciate everyone being punctual in returning to the room after the break.

So with that I'd like to introduce our current panel which is First Responders Using Broadband Technologies to Advance Public Safety. And this panel is examining how the National Broadband Plan should reflect the current and potential uses of broadband to improve public safety communications and operations, including the utilization of the Internet and web-based applications. The panel will also examine issues that impact broadband deployment and/or technologies in the public safety arena, such as interoperability and cost and infrastructure limitations.

And I'm going to introduce our panelists and the FCC and other U.S. Government

participants. But before I do I wanted to just ask our panelists to please say "next" fairly loudly when you want your slides and Stephanie, who is sitting in the back, will be the person who needs to change the slide. Ronnie Cho up front is timing you so you have five minutes. I will cut you off nicely. And then what we'll do is we'll open the floor to questions both from the U.S. and FCC participants on the panel and then from our floor. And Tim May over here is handling any questions that come in from the web. So we're hoping to have a very lively discussion.

So with that, I'm only going to introduce people briefly. Their full bios are in the guide that you got this morning in the program.

So with that, next to me is Charles Brennan, who is deputy secretary, Commonwealth of Pennsylvania's Office of Public Safety Radio Service.

Beside him is Mr. Stephen Carter, who is the vice president of Technology at Qualcomm.

Next to Stephen is Pete Eggimann, who is chair of the Operations Committee at NENA and also director of 911 Services for the Metropolitan Emergency Services Board in St. Paul, Minnesota, and also was a Next Generation 911 trial participant.

Ralph Haller is sitting next to him, who is chair of the National Public Safety Telecommunications Council.

Next to him is Glenn Katz, who is president and COO of Spacenet, Inc.

Next to Glenn is Harlin McEwen, who is chair of the Public Safety Spectrum Trust.

Adjacent to Harlin is Bill Schrier, who is the CTO and director of Information Technology in the City of Seattle. He's here representing APCO.

Next to Bill is Laurie Flaherty, who is a program analyst at the Office of Emergency Medical Services at the National Highway Traffic Safety Administration at DOT.

Next to Laurie is Jeff Goldthorp, who is

chief of the Communications Systems Analysis Division of the Public Safety and Homeland Security Bureau here at the FCC.

Next to Jeff is Charles Hoffman, who is chief of the Disaster Emergency Communications Programs at FEMA.

Next to Charles is John Leibovitz, who is deputy chief of the Wireless Telecommunications Bureau here at the FCC.

And next to John is Kathryn Medley, who is chief of the Satellite Engineering Branch and acting chief of the Systems Analysis Branch at the International Bureau at the FCC.

Erica Olsen is sitting next to Kathryn. She is special counsel at the Public Safety and Homeland Security Bureau.

And next to Erica is Dan Phythyon, who is chief of the Policy, Planning, and Analysis Division at the Office of Emergency Communications at the Department of Homeland Security.

I want to thank you all for appearing today. And with that I'd like to turn the floor

over to Charles.

MR. BRENNAN: First slide, please. Good morning, everyone. Next slide. The first thing I want to show you is Pennsylvania's network. That's the network we built for our radio system, 800 megahertz digital voice over IP network in Pennsylvania because in the end broadband is about networks.

Right? Next slide. That's a composite of what we believe in Pennsylvania to be areas where wireless data coverage exists by commercial carriers. You notice the large swabs of white areas where there is no coverage. Also, we believe to the best of our knowledge that that is probably overstated. There are probably a lot more areas in Pennsylvania that do not have coverage. So it's not only about where the networks exist where we can build networks, but where networks do not exist and public safety may not have wireless broadband coverage.

I want to concentrate -- next slide, please -- largely on wireless. Even in the more

remote parts of Pennsylvania, the PSAPs all have broadband. Hospitals have broadband; schools have broadband, where I think broadband is most important is to the vehicles -- to the first responder vehicles in the field. So I'd like to concentrate just for my few minutes left here on wireless broadband.

Although it's great to say we'd like to have broadband everywhere in Pennsylvania and everywhere in the United States for first responders, our goal in Pennsylvania really is to look for more hot spots where we would have broadband. Be able to drag it where we need it. Situational broadband. Broadband to be used in emergencies.

Pennsylvania will have such an event approximately one month today. The G20 Summit is coming to Pittsburgh. We intend to put our broadband in downtown Pittsburgh for public safety use there. That's a good example of, I think, where public safety will probably first move with broadband more situational.

I showed you the commercial map there. The reason I think that it's unlikely broadband will be available everywhere is that in a lot of those places there's only a single commercial carrier. And when that happens, when there is no competition, public safety pays a lot for broadband. And public safety and government, in general, doesn't like open cost. Per megabyte cost for wireless. We like fixed cost because it fits nicely into how we budget.

Where also Pennsylvania is moving is in the next bullet -- is we're viable state networks which can be built -- can complement commercial carriers. As a matter of fact, Pennsylvania is moving in that direction now with our latest stimulus grant--Broadband Stimulus Grant. $7.2 billion in stimulus funds for broadband sounds like a lot of money; in the end it's a drop in the bucket. We all know it's not going to solve the problem, but we have to use what we have.

And no one likes these big ugly towers in their neighborhood, so we might as well

concentrate as much as we can on the big ugly towers that we have. And that means co-locating commercial carriers with state networks. And that's where Pennsylvania is actually moving.

I'd like to just talk for a minute on grants. A lot of broadband for public safety is going to be implemented via grants. The grant process for those of you in the public safety realm in government, you know how horrendous that it is. Competitive grants, I don't believe that if we want to get these monies out to public safety, get these networks built, competitive grants are not the way to go. Block grants to the states. Let the states control where those monies go. Too much money is being filtered down to the locals and frankly, I think, being waste. As you know, about 80 percent of the money has to go to the locals. Very, very difficult to manage a statewide vision when you're giving money to all these different local organizations who may not have the vision for what is best for the most.

Also, rather than competitive grants,

block grants. We spend an awful, awful lot of time filling out paperwork for competitive grants. I'd rather see the money block granted to the state and all the money that the grantor is going to use to administer the grant and check all our grant requests, I'd rather them use that money to hire staff to help us manage the grant. So I think block grants are the way to go.

Also, it's not just about the PIPE. It's not just about the broadband; it's about the applications that go with it. I was asked a question recently by someone who should know better and said, "Why do I need broadband?" A public safety person, "Why do I need broadband?" Public safety really doesn't understand what they need broadband for, and I think that's more on the vendor to help them understand what they need.

My last point is there's got to be a greater focus on data interoperability. After 911 it was all voice, voice, voice. Data, there's a lot to be said for data. Look at Twitter. All it is is a couple lines of text and look how much you

can say with text. So, I think we, as public safety, have to look at more data interoperability, grants for data interoperability, and how it can be used for public safety purposes.

I have 10 seconds left and I made it. Thank you.

(Laughter)

MS. MANNER: Thank you very much. And you set a very good example for the other panelists.

So with that I'd like to turn the floor over to Stephen.

MR. CARTER: Thank you, Jennifer. Good morning, ladies and gentlemen. My message today is simple and brief. It is that as we embark on this challenge to get a nationwide interoperable mobile wireless system for first responders, we have a lot of challenges. The challenges will be in the areas of rollout, funding, regulatory policy, all of these things. But the thing that will be the least of the challenges is actually

making the commercial technology fit for what we need it to do for first responders.

Next slide, please. Depending on who I'm talking to, that statement that today's commercial technology will fit the needs of first responders very, very nicely, it's either patently obvious, usually with a joke about their kids having better technology than they do at work, or it's an absurd statement that how can a commercial technology actually meet the needs of systems that were traditionally designed from scratch specifically for first responders. But the key is that even in today's 3G commercial cellular industry, the underlying primitives -- the building blocks, if you will, for what public safety needs to do -- are all there. All of the Voice Over IP, the high-speed streaming data, the support for tiering of different levels of services and quality of service and location-based services, it's all there.

And just as we see in a lot of the high-end Smart Phones today, the ability for

public safety to take those underlying building blocks and use them to build their own applications and their own custom uses is going to be very straightforward.

Next slide, please. And, of course, we're embarking on the transition in the commercial world from 3G to 4G, and we're pleased to see that several of the major public safety industry groups have endorsed LTE as a way to move forward for the technology for public safety. It's going to be an evolutionary change; not a revolutionary change. Excuse me. And that's important, both for the commercial world and for the public safety world, because to do an efficient rollout -- to get widespread coverage rapidly and inexpensively -- we're going to need to worry about that kind of gentle upgrade and backward compatibility with the 3G networks.

So we'll get a little bit better spectral efficiency in the inner cities. We'll get a little bit fatter PIPE. But in general, the commercial technologies that are here today are

just going to keep working as we move forward to 4G and will serve public safety very, very well.

Next slide. So, as this begins happening, as we debate all the regulatory and rollout issues, the things that we really -- that I really recommend we keep in mind are, first of all, keep the focus on the policy and operational issues of how we're going to use this technology. In past years we've spent an awful lot of effort debating whether this can ever work or is it crazy for commercial technology to be shoehorned into a public safety role. I'm pleased to see we're getting past that because every time we look at it we find that any issues that people perceive that the technology won't work really end up being business issues and deployment issues of commercial carriers today, not the fault of the underlying technology and how we would use it in a public safety fashion.

Second, this question of whether this is going to be mission critical, whether it's appropriate for mission critical or whether

broadband needs to maintain kind of a secondary status as a backup tool for public safety, doesn't need to be debated too much because, again, the issue is one of rollout and deployment. If we build the system out to a quality of service, to a redundancy level, to a backup level -- generators and such -- for mission criticality, it can be used that way. If we build it out like commercial vendors have, then we can't. It's our choice.

And third, one of those particular debates about mission criticality has centered for a long while over the question of how this new broadband network will interoperate or should interoperate with traditional voice dispatch systems. We don't need to debate that right now. The commercial world likes to do gradual and evolutionary upgrades also, and the way they're doing that with LTE is to utilize it first for data. It has all of the hooks in it for Voice Over IP, and some day commercial carriers will be doing what they would call mission critical voice over the LTE networks. But they'll make that

decision down the road.

And I would argue that we can make exactly the same decisions down the road in public safety. We can deploy the system first for the data needs that we have today and are not being met, and down the road figure out the right way to interoperate with existing mission critical voice systems.

Thank you.

MS. MANNER: Thank you very much, Stephen. With that I'd like to turn the floor over to Pete Eggimann.

MR. EGGIMANN: Good morning. Next slide. The concept that I want to talk a little bit about this morning is -- I want to use the example of what we're working on in the Minneapolis-St. Paul area. And my focus in my real job as I call it is trying to transition us from the Legacy 911 system that we know today to a Next Generation 911 system. We believe that in order to do that effectively in our area, that we need to link our centers together throughout the

metro area on a wide area network.

Go ahead and go to the next slide. Kind of a brief map here just shows the counties in the Minneapolis-St. Paul area. We work for eight of them. The red dots there are the 911 centers in each of the counties. The stars in the middle would depict the data centers where we would house applications. And the black dots there are city-operated PSAPs that at some point we would connect to the line connecting the red ones there, the wide area network.

Next slide. The idea behind the public safety network as we call it is that we want to create an environment where all of the applications that the call takers or dispatchers would use can reside at the data centers and therefore would be available anywhere that they signed on to the network.

We want to create a converged environment where there's no separate silos, so to speak, or separate -- we don't believe that we can create a separate broadband network for every

application. It would be like, you know, having a computer for word processing and having another computer for e-mail, and another computer for e-mail, and another computer for Excel. And that's traditionally the way we've done it. And we've also built systems out at the PSAP level. We don't believe that we can continue to do that as well. We need to do this at a regional level and share this network across applications. In our example we believe that we're going to need about a 1 gigabyte Ethernet ring connecting those county PSAPs and those data centers together to handle all of the application band width.

Just for a context, the Minneapolis-St. Paul area has about 2.7 million people, about 189 on one answering positions. We process between 1.3 and 1.4 million calls a year, and over 50 percent of our wireless calls are now -- over 50 percent of our 911 calls are now coming from wireless devices.

Next slide. In the past, interoperability has almost always been used in

terms of wireless or in terms of radio communications. I would submit that interoperability needs to really focus on applications. The information that we receive--we need to be able to pass on to the responders. We need to be able to share it with the people that assist us. Those applications that they use -- it isn't realistic for us to all use the same application. We'll never get everybody to agree on that. So the interfaces between them need to be open. They need to be standard space so that we can move data back and forth without conversion.

In the example that I've got up there, if you read through that sequence and you get down to the bottom, you're actually going to realize that the call taker never actually has to say anything in processing that call. They need to make sure that it's happening. They need to monitor it. They need to make sure that the other agencies have received what they've gotten, but they don't have to actually say anything. There

probably would be an additional hook in that scenario that would allow the EMS and the ER to actually get the patient's records from the patient's home doctor.

Let's go to the next slide. I'm just going to close it up here with we really need to work together here to leverage the resources. Internally all of these things can be managed at a regional level. The external side of this is that it's easier for carriers to connect. They're connecting at two points rather than at 19. We can share the routing resources, those kinds of things.

The bottom point there is that this is scalable. This can be replicated across the country. It would allow us to deploy Next Generation 911 very quickly and ubiquitously.

And I'm over. Thanks.

MS. MANNER: Thank you, Pete. I appreciate that. Ralph, it's your floor.

MR. HALLER: I'm Ralph Haller, chair of NPSTC, the National Public Safety

Telecommunications Council. It's an organization of -- umbrella organization of about 15 public safety organizations. One of the things that we're working on now is to decide how broadband fits into public safety.

Next slide, please. I start out by saying it's really all about moving data, whether it's medical EMS information, firefighting, robotics, automated inspections, intelligence gathering, environmental monitoring, collaboration of resources -- for example, between PSAPS -- surveillance, traffic management, access to law enforcement databases. It's all about getting data to the people that need it in a timely fashion.

Next slide. From an operational standpoint, a broadband network has to provide Internet access and that's wired to wireless to wired. It needs to be seamless access across whatever entry point you have into the broadband network. There needs to be connectivity between networks, broadband, private land, mobile radio,

satellites. The network needs to provide virtual private network capabilities so that anywhere that someone needs information they essentially can have their desktop, whether it's in their squad car or whether it's helping foreign PSAPS somewhere, they need to have access to the home networks. It needs to provide messaging for mobile, and it needs to provide location information, and it needs to provide access to land mobile systems.

Next slide. It also needs to provide multiple modes: Voice, data, video. It needs to have a strong backbone for connectivity. It can be used to move data between points as a backhaul system or as an information system. It needs to have access to the Public Switch Telephone Network. It needs to be able to dynamically create little networks as events occur and small networks in a localized area need to be set up. It needs to have that capability. Provide security, authentication, and encryption. It has to be survivable and reliable.

Additionally, it has to provide service in remote areas. I'm particularly concerned about that. My sort of full-time job is executive director of the Forestry Conservation Communications Association. All of the work that our members do is basically in the forests of our country. And so we have a particular concern that broadband be available not only in the big cities but also in the rural areas because it's just as important for a firefighter on a forest fire as it is for a policeman in a city.

And I also want to point out that we do not consider broadband to be a replacement for traditional land mobile dispatch radio systems. It will augment them. We don't see it will replace them for a number of reasons, one of which is 700 megahertz isn't effective in all areas. It takes a lot more infrastructure in some areas. And so the traditional dispatch systems at VHF and UHF we consider they will be in use for a long term.

Next please. For wireless systems, the

public safety community has generally set it on LTE. I'm not going to go through these in great detail but basically there needs to be dynamic bandwidth assignments so you can prioritize. If you've got a specific size PIPE you need to be able to prioritize what information goes across that if there's a contingent for resources. It has to provide user authentification; handoff between networks; access to applications, be it mapping, documents, whatever.

Next slide. For governance, the network needs to have standards that are national. Public-private partnerships should be permitted. Public safety should have priority access on spectrum, shared spectrum, and bandwidth management is a priority.

Next slide. Finally, what can the FCC and Congress do? In terms of wireless, the FCC can issue rules for national-local build out and issue waivers in the interim. The FCC can allow the public safety broadband licensee to sublicense to regions. The D Block needs to be made

available to public safety in some manner. Congress and FCC should allow national and public-private partnerships, and also allow access to all responders including critical infrastructure.

My last slide, please. What else? Funding. Access to perhaps the Universal Service Fund, grants for broadband development, spectrum auction proceeds. And how about tax advantages for carriers that provide public safety support? Also, how about resource sharing? The federal government has never been very open with the resources it has in place, and we think there's probably a lot out there that could be shared among state and locals that needs to be explored.

Thank you.

MS. MANNER: Thank you, Ralph. With that, I'd like to turn the floor over to Glenn.

MR. KATZ: Thank you very much. I apologize. Some of these slides have some animation, so if you would just click through until the animation finishes on the particular

slide when I say next slide. Okay?

MS. CACCOMO: I'm sorry?

MR. KATZ: I said these slides have animation on them, so if you would just click through so we can get through it.

Thank you very much, everyone, Jennifer and James. In the next few minutes I would like to hopefully define the role that satellite communications plays within a broadband national infrastructure plan.

Next slide please. Okay, next slide. Sorry. Go back one slide. Okay.

So I'm going to first address who are the constituents or customers; what are their needs and challenges; what solutions exist today; is there a best practice example, and there is, which I hopefully will be able to discuss here shortly; and what do we recommend going forward for the FCC and other policymakers?

Next slide, please. There basically are -- if you would continue to click through on this one -- there basically are two different types of

needs that we call emergency management under broadband-type of conditions. One are for first responders, people who have to be on-scene in minutes and deployed for several hours, and, of course, there are the what we call relief deployments, where a solution has to be on scene or communication network has to be put up in hours and has to stay there for weeks. The types of constituents that you see on this slide I think are familiar to all of us.

If you just click through again that would be helpful. Continue. Right.

These are the types of constituents that you see on both sides of the needs columns.

Next slide, please. Please click through. There are six basic technical challenges that we see in this, with this problem or challenge relative to broadband communications. They are the ability to provide voice, video, and data seamlessly over the same network. The systems have to be deployed in a rapid manner. They have to be easy to operate. They have to be

secure; the communications themselves have to be secure. And it has to be very, very high quality equipment that has to be out there. It has to be interoperable; we've heard that from some of the other panelists. The solutions have to be integrated, integrated with either the local network or the Land Mobile Radio-type network that's out there for these public safety responders.

And fundamentally, if there's anything -- there's a lot of information that's being put out here -- but if there's one single thing that all of us as industry experts and policymakers can take away from this to help guide us as we continue down this National Broadband Plan, it is that our job as policymakers and industry associates is to minimize the complexity for our public safety workers so they can focus on their mission. They don't have to be out there messing with communications equipment or trying to consider where they're going to get funding or what their bandwidth needs are and how they're

going to set this equipment up.

Next slide, please. There are solutions that already are out there.

The good news is from an industry perspective, I believe since Katrina in 2001, we have made strides in being able to provide what I would call equipment and services that are available also at reasonable costs, if you will.

Next slide. I want to talk a little bit about a best practice example. So, I'm under some nondisclosure situations with this client of ours, but it is a very large public service organization, a large metropolitan police organization. They have a terrestrial network in place, obviously, but their biggest challenge was they needed to provide 100 percent availability all the time at all their precincts and all their data centers regardless of whether there was a disaster, natural or unnatural. To do that they needed to have an overlay network to the terrestrial network, which obviously has to be satellite-based. It has to be totally diverse

from their terrestrial infrastructure. They also required that it be integrated seamlessly within their existing IT network which was quite complex and had to carry both voice video and data. It also had to have -- the antennas had to have a resistance to very, very high winds, assuming there was a hurricane-type situation that may come through the locality.

What was the solution? We took a satellite network. We overlaid it. We created some very, very high resistance antennas and reintegrated the satellite system within their Cisco-based IT network. What did they get from that? They got obviously a total network backup solution with 100 percent availability that is working today.

What's the key to this, which I'll go into my next two slides for the recommendations? The key to the entire thing was not the technology; it existed today. It was funding. They were not able to get funding from their own budgets. They had to go to the federal

government. The federal government gave them a grant. This is great but do you know what? There's a lot of other localities and organizations like this in the United States that do not have this capability. And if there's a disaster of any type, natural or unnatural, they will not be able to communicate, which means our public safety people will not be able to do their job correctly. That's the message here.

If you go two slides, please. Next slide. What do we recommend? We recommend that from a policy perspective we do agree with most of the other panelists that say it needs to be state-generated as opposed to from the localities. The grants need to be taking in block grants to the states. And if the states can coordinate with all of their other constituencies a plan that will take in both public safety, other anchor institutions under one sort of state broadband plan for emergency management, we think that's the most efficient way to do that. Obviously, to do that the federal government, the policymakers have

to make the right policies and the federal government has to be able to fund these types of services.

Thank you.

MS. MANNER: Thank you. Glenn. With that I'd like to turn the floor over to Harlin.

MR. McEWEN: Thank you, Jennifer. I'm pleased today to be representing the Public Safety Spectrum Trust, which is an entity consisting of representatives of 15 national public safety organizations.

Can you go to the next slide after that? Next slide. Thank you.

Today in public safety communications, and for all of my career for the last -- I won't go into that -- many, many years, we have been based on voice centric communications. And while voice will always be critical to public safety, we're moving now to data centric communications as an important part of our communications portfolio. We need to be able to have access to broadband services, both wireline and wireless, to be able

to provide those kinds of services that public safety is urgently in need of.

Over the past 10 years we've moved from slow narrowband data to wideband data and now broadband data.

Next slide, please. So, during this period of time, we have been currently, you know, limited to commercial wireline and wireless broadband services, something which we're trying to do differently in the future.

Next slide. Public safety, as I said, should be able to deploy Next Generation, in other words, fourth generation. We're now in third generation high-speed wireline and wireless data services that give us not only secure text messages but documents, photographs, diagrams, and streaming video. Our vision is to have broadband for public safety everywhere. We need to have broadband that's brought to us by wireline and by wireless services, both terrestrial and satellite. It has to be a total delivery. We need to have those delivered every place that we are. And

that's something which is a vision that we have for the public. In other words, our vision of shared spectrum for public-private partnerships should also bring broadband to unserved areas of the country.

While we are working to bring us those services everyplace, we should be able to also assist in bringing unserved areas broadband.

Next slide. So the public safety goal is to have access to a seamless broadband system that includes the last mile of reliable wireless broadband service as envisioned in the currently proposed 700 megahertz national public safety wireless broadband network. The wireless broadband network should include broadband data services like I mentioned with things like text messaging, photos, and streaming video. And we need to be able to support the Next Generation 911 and public safety services. You'll hear about that a little bit from Laurie; you heard a little bit about it from Pete. But this is one of the big issues, is that 911 services are somewhat

antiquated with old technology. We need to be able to support that along with other mobile services for the next generation of public safety.

We need a hard and public safety network with infrastructure built to withstand the kinds of local and natural disasters like tornados, hurricanes, earthquakes, floods, and so on, and this is the kind of thing that we build in our current voice public safety systems. I always give credit to the commercial services who are quite rapidly now beginning to bolster their services to give them the kinds of things that we expect. Unfortunately, that isn't all there yet.

Next slide. So we need nationwide roaming and interoperability for local, state, and federal public safety agencies -- that's police, fire, and EMS -- and other emergency services, such as transportation, health care, and utilities. We need access to the Public Switch Telephone Network similar to what is currently available in commercial cellular services. We need Push-to-Talk, one-to-one, and one-to-many

radio capability that would provide a backup but not replace traditional public safety land mobile mission-critical voice systems. And last, we need access to satellite services to provide reliable nationwide communications where terrestrial services either do not exist or are temporarily out of service.

We, at the Public Safety Spectrum Trust, look forward to working with the FCC to make sure that the National Broadband Plan includes information relative to the urgent and unique needs of public safety.

Thank you.

MS. MANNER: Thank you very much, Harlin. And last but not least, Bill.

MR. SCHRIER: Thank you, Jennifer. I'm Bill Schrier from the city of Seattle, and I'm here today representing APCO International, the world's largest organization dedicated to serving the needs of public safety communications professionals with 15,000 members. I'm also one of the few people you'll hear from in all these

workshops who represents the cities and counties of America.

The cities and counties have the 911 centers, control the rights-of-way, and employ the first responders of America.

And I bring you today a vision for fibering and unfibering America.

Next. America's networks, the ones we have today, lack sufficient bandwidth. I believe the goal of the broadband plan should be a fiber optic network to every home and business in the nation, coupled with widespread private and public safety fourth generation wireless generation networks.

And you've already heard about that from the other panelists.

Next. If you look at the history of the United States, we've built these networks before. The telegraph, the electrical network, the telephone network, public safety radio, cellular telephone, the national highway infrastructure. We built national networks before. They made us

more safe, more secure, and more economically viable as a nation.

Next. The new technologies we've seen explode on the scene in the last few years have great potential. Clearly, the United States created the Internet. We've got web. We've got e-mail. The FCC, as a matter of fact, has led the charge for the digital TV transition. We now have HD television, at least for broadcast. We've got amazing applications, such as Facebook and Twitter, but we've not harnessed this technology for public safety. There is insufficient bandwidth.

Next. As Admiral Barnett stated in his opening remarks very eloquently, 911 and 311 have great potential. Video calls, HDTV, cameras are everywhere. In Seattle, for example, there's a video camera in every police car. Gee, most people in the United States now either carry or have the potential to carry a device like this where you can actually take a photograph, if I can take a photograph, and e-mail it wirelessly. But

our public safety responders can't receive it. They can't receive video that's taken by these devices that are carried by many Americans.

Why? Again, it's because of insufficient bandwidth and insufficient networks.

Next. So, my recommendation--build fiber to every home and business in Seattle. There's at least 111,000 households in the United States. There's at least 22 million -- 111 million households in the United States and 22 million small businesses in the United States. It's a daunting task. In the meantime, we can also fiber PSAPs, 911 centers. And when you've got fiber there -- this is a map of Seattle, incidentally, with our existing fiber -- when you've got fiber to every one of those neighborhoods, you can pop up wireless access points. And lo and behold, you can also have a fourth generation wireless network.

Next. Such a network -- such a fiber network would not only be useful for public safety, but it would have a wide variety of

civilian applications that would make America more secure. Telemedicine, tele-education. Think of your children, for example, actually being educated in their home and attending classes from a university or a college actually in their home. Every home or business is potentially a video source with such a fiber network.

Next. This also has great environmental and homeland security implications. We can reduce automobile trips. We can reduce traffic jams and lost productivity. We can have true telecommuting. Rather than having me fly 3,000 miles across the country from Seattle burning jet fuel, you could actually see me in HDTV video if there was fiber here and if there was fiber in Seattle. Think of the implications for the reduction of our dependence on foreign oil if we can all of a sudden do that as opposed to commute people all over the nation.

Next. Again, this is a daunting task. I've talked about 111 million households. I've talked about our many millions of small businesses

and other premises. But the technology is here. And what I urge you and the FCC to do with this National Broadband Plan is exercise the same leadership and bold vision you've exercised in the past on wireless and wireline networks, and challenge the United States of America to build fiber to every home and business and then pop up fourth generation wireless networks on top of that.

MS. MANNER: Thank you very much, Bill. Well, thank you first to all our panelists for their presentations. They were very interesting. What I'd like to do now is first open the floor to our FCC and government participants if they have any questions, and then we've already been receiving questions via the webinar. So we have some folks there. And also open the floor to folks here in the audience. But I would suggest that anyone who asks a question--I would ask that you introduce yourself when you state your question.

So with that, are there any of our

government participants? Jeff?

MR. GOLDTHORP: Thanks, Jennifer. I have a question. I think it's directed to Mr. Carter, but I think others might have an idea, too, about what I'm suggesting.

And what I heard you say is that you think the commercial technology can basically support the needs of public safety and left the question of provisioning a little bit up in the air in terms of who does what to actually make the commercial technology available to public safety, whether it's provisioned the way technology is currently provisioned for public safety through private network or whether it's provisioned through a commercial rollout by a commercial carrier or some combination of the two.

And so my question is in your mind do you have a roadmap, really, a plan, for how you see the commercial technologies that you've described actually being made available to public safety users, whether it be by commercial providers or whether it be by private providers?

Because I didn't see that come across clearly. And if it's something that you have additional thoughts on I'd like to hear about that.

MR. CARTER: Certainly. Well, that's the very big question, isn't it? A lot of money is going to be spent doing some sort of rollout for public safety, and with a lot of money comes a lot of questions.

I would not go so far as to say that public safety's needs should be met entirely through provisioning service to them through commercial carriers. They can do that today. For many it makes a lot of sense. Many local police, fire, other agencies, contract with their local cellular carriers today to get service. As a national model, that probably falls short.

We at Qualcomm, we're very big fans of the public- private partnership and the D Block auction that was attempted. For a variety of reasons that didn't work the first time. We'd like to think that it could work a second time because it would provide the needed funding to

deploy the system. Absent that we're going to need to find some other deployment, some other funding mechanism for a public safety-only system.

So, some combination of the rules changes of what happened the first time with public-private partnership might be a good way to proceed. But beyond that I think it would take much more than the time we have today to nail down specific rule changes to make it work.

MR. GOLDTHORP: But do you have -- for example, you implied that commercial technology can meet the needs of public safety today. Do you have anything that stands behind that statement?

So, for example -- I'll give you an example. PTT call set up time. What is it -- do you have -- are there deployments where, say, 3G networks or LTE networks have been deployed with PTT call set up time that public safety entities would consider to be acceptable?

MR. CARTER: Certainly. And that's actually a very good example.

Sprint today offers a variant of PTT

that we helped them developed. It took several years because of the problem you're describing. Initially, Push-to-Talk technology on the cellular network was not nearly a fast enough response time to compare with the purpose-built systems either for public safety or the original Nextel Push-to-Talk system. Once the changes were made to commercial CDMA cellular, Sprint was able to deploy service that users didn't see any real difference between the old Nextel Push- to-Talk service with a virtual instantaneous Push-to-Talk and the newly deployed CDMA system that was put alongside it.

I'll leave it at that. That's one example that you requested, and I think in other areas the technology that's used commercially -- maybe if you bought it today at your local carrier store -- would not come with service plans and provisioning and service guarantees that meet the needs of public safety, but by and large whenever we go to look at examples like that we find that it's business issues, not --

MS. FLAHERTY: This is a question perhaps for Mr. Haller or for Mr. McEwen and others.

In the DOT Next Generation 911 project, our mantra has been to begin with the end in mind. And what I mean by that is providing the data to the first responders that would be useful to them, that is actionable, that would actually make a difference in terms of making their operation more efficient or their jobs easier. It has been our impression thus far that those end users have not been adequately engaged to decide what data they want. And I'm wondering if you have had the involvement of those folks in deciding which data they feel would be the data that they want transmitted to the PSAP and onto the first responders.

MR. HALLER: I think it's a very good question, and I would respond by saying it's an evolutionary process. In some respects people don't know what they want until it's offered. You know, if you take the telephone, basic telephone,

people survived for centuries without it. Once that capability was there, they suddenly couldn't live without it. I think the same thing is going to be true in broadband. They're seeing capabilities through the Internet right now and it's going to be an evolutionary process for people to say I need; this for suppliers to say you can do it in the following manner. I think it's very hard though for somebody, a first responder, to sit down and say here's a list of 25 things that I absolutely need at this point. It's going to be evolutionary and the network is going to grow and expand in its capabilities with time.

MR. McEWEN: Well, I think your concern is interesting. First of all, I do believe that there's a lot of engagement in the public safety community to determine what their needs are. The current NPSTC Broadband Task Force has been looking at the applications that are necessary and you probably haven't seen that yet because it hasn't been released. They're in the middle of that.

Obviously, thousands and thousands of public safety officers, firefighters, police officers, EMS officials, and so on are not intimately engaged in this process at the moment. But the fact is that the national organizations that many of us represent -- the Police Chiefs Association -- we have committees made up of people that represent our membership all over the country that are engaged actively in those kinds of things.

So I believe that we're actually doing pretty well in defining what it is we need. My concern is that the application part of it will be, you know, like said, kind of an evolution. But at the moment, if we don't have the broadband service, wireline and wireless services to get it to them, it really doesn't make much difference because it just doesn't get to the people that need to get it.

MS. MANNER: Thank you, Bill.

MR. SCHRIER: And I'd like to make a practical comment on that as well.

In Seattle, as I mentioned, every policy vehicle has got a digital video camera in the vehicle. And whenever there is a car stop, that car stop is recorded in the digital video, but it's recorded in the vehicle because there is insufficient bandwidth in the wireless networks to be able to transmit that. Think about the safety of the officer and the citizen if all of a sudden the dispatch center, the 911, could see what's happening on that car stop in real-time. Or better yet, the officer's sergeant could see what's happening in that car stop in real-time, or other officers in the field. That is one application which, because we have insufficient bandwidth, both officers in the field and 911 centers could see an immediate application for.

MS. MANNER: Thank you. Any other questions? Dan?

MR. PHYTHYON: Thanks. This goes to some of the comments I heard earlier on grants policy. I think I heard several of the panelists talk about to the extent we're moving forward and

grants will continue to be a funding stream for broadband applications, it's better to direct those at the state level in block grants and what have you.

Our office has some grants responsibility. I know that Laurie Flaherty's office has it as well. I'm curious. Some of those who perhaps represent more of the local constituencies, do you agree with that? Or what are your thoughts on the -- kind of the proper direction of grants from a federal perspective?

MR. McEWEN: I'll start. Because I represent every level of government from small local government, to country government, to state government, and to federal government, and the Police Chiefs Association, we have to look at it in a very broad way. So, there are lots who believe that the funding should not be controlled by any one group. It should be kind of available through a varied way of distributing those monies. There are people in state government who believe that they ought to control those funds. Most

local governments do not agree with that. They want that money to be available directly to them. So, it's a difficult thing for us but I believe that it ought to be a variety of different ways of delivery.

MS. MANNER: Go ahead, Charles.

MR. BRENNAN: I came from a local, a big local, and now I'm with the state. And I can tell you that my state view has really changed my opinion somewhat.

Because what I can see is that a lot of the locals can't run a technical grant, especially the complexity of some of the systems that we've asked them to put in. They just can't do it. And we end up giving them the money. They control the money but they need us to hold their hand in order to do the grant and we don't have control over that. And, you know, also when you shove the money down to the local -- I hate to say it, but, you know, the locals look for me -- for the locals. Not for the greater good. And I have found that the state -- I know this is hard for

people to believe -- the state does look for the greater good, the greater good of the state. At least that's my opinion.

But I think we have a better purview of where the money can go. We have the technical resources to help the locals get through some of these very, very complex issues. These LMR Systems and all have gotten just extremely complex in the last couple of years to put in. Microwave fiber, all the software, the radios are all software defined now. Much different animal than they were like 20 years ago when I got into the business. So I think that's one reason why I think you want to keep it at a higher level.

MS. MANNER: I think Pete wanted to add something in.

MR. EGGIMANN: Yeah, I guess I'm somewhere in the middle on this. But I think you need to scale the grants to the project that you're trying to accomplish. The regional concept that I talked about, and I said that that's scalable.

That could be a state project; that could be a five state project; that could be a county, you know, a group of counties as we're talking about or looking at in Minnesota. But if you do it at some sort of a regional level you tend to level out the haves and the have-nots. And, you know, if you go to -- at the agency level, I'm afraid that you're going to end up with, you know, the big agencies that have some resources are going to move forward very quickly and you're going to leave some of the rural areas behind.

MR. KATZ: I'd like to make a comment as well. Besides the process to get grants to local government sources or state, there's also an economy of scale that we can't lose sight of. So if we're -- until the time we get fiber out to every single locality so the bandwidth is there, you can imagine a situation where there is a pool of bandwidth as opposed -- each locality needs X, let's say, megabits per second. We're all engineers here, right? And that's what they're

going to buy and try to purchase with their dollars.

But if you had a situation where you could aggregate X megabits per second that can be distributed in real-time on demand to several localities when they need it -- as an example for emergency-type situations -- you create an economy of scale that I think is required here in this type of situation. Hence, the idea to have it state or regional--that's another idea. To pool bandwidth to be used in an economical fashion but give the locality what they need from a bandwidth perspective when they need it.

MS. MANNER: Thank you. Erica, you had a question?

MS. OLSEN: I do. I actually just wanted to follow up on some of these comments relative to bandwidth and what you actually need. I think everybody in the commercial world or in the public safety world would tell you we need more bandwidth. Well, tell me how much is more? You know, how do you justify that? Have you done

the studies and you're telling me you may not necessarily know what applications you might want to ride over this--how do you figure out how much is more, especially when we're dealing with a limited resource both in terms of the spectrum or the capacity itself and the funding to get that capacity available?

MS. MANNER: Harlin?

MR. McEWEN: I'll start. More is definitely different than where we are today. We right now have only -- in public safety until this broadband is resolved in the 700 megahertz -- right now the only spectrum that's available is narrowband spectrum and that spectrum brings very slow speed data. You know, 96 kbps.

MS. OLSEN: That's not necessarily true.

MR. McEWEN: We're talking about being able to, you know, provide higher speed data services.

MS. OLSEN: You do have 50 megahertz at 4.9, which is broadband.

MR. McEWEN: But it's not practical for

wide area networks. I mean, I've been told -- I'll give you the example and probably somebody will take me to task on this but I'll use it anyway. We were told that somewhere around 37,000 sites are necessary to build out 700 megahertz to the degree that we would like in this country. To do that with 4.9 they tell me it would be 60 million. So, if somebody wants to figure that out on an envelope, do so. That tells you it just isn't practical for wide area data.

MS. MANNER: Bill?

MR. SCHRIER: So I'd suggest 6 Mbps, which is a HDTV stream uncompressed. And if you want that to be two- way, 12 Mbps. If you're going to have multiple HDTVs in a home or a business, multiply that by, if there's three of them, 36 Mbps. But you've got to think two-way and symmetrical, but those are the sorts of speeds that we're talking about. Now, certainly you're going to apply compression algorithms and other things to those streams and perhaps get them down, but that's the sort of bandwidth we need.

Two-way, HDTV, multiple streams to any given location, fixed or mobile.

MS. MANNER: Charles?

MR. BRENNAN: Let's stick with wireless for a second.

I would tell you coming from the public safety world, actually, most of the public safety applications use very little bandwidth. If you look at what they tend to need, they need access to the National Crime Information Center, wants warrants, missing persons, stolen cars, state databases, local databases -- largely text-based that fill in screens that are already on the mobile data computer. Most of them are happy with that, especially those that don't have it. I mean, when we gave our state police access to all that stuff, they think it's fabulous. Give them access to small photos that run over 19.2. I mean, we paint a screen with a small photo. They're very happy with the photo.

Again, coming from public safety everybody talks about streaming video out the

patrol car. I see less of a need for that to be honest with you. Do you really want the cop looking at a streaming video while he's moving along at 60 miles per hour? And they will do it. Having put mobile data computers in a car in a big city in Philadelphia, I could tell you how many of my cops ended up in the truck of the car in front of them, you know, while they're looking at the mobile data computer. So I'm more for static photos. Situational broadband I think is a big deal. I'm very much in favor of that. But these large PIPEs out to the cars -- in the future, yes.

I think the big future application for law enforcement is transportation of fingerprints wirelessly. That is a big deal for law enforcement. One of the most difficult things for the cop in the field is to know that the person he has stopped is the person who he says he is. That is very difficult. Yes, he's got a license. Yes, he's got a picture on the license, but who is that person? That is very difficult for law enforcement to ascertain. And right now all they

have right now is yeah, you have a name. I plug in your name. You are who you say you are. Go on your way.

I think the future is fingerprints out to the car; wirelessly transmitted back. The FBI has gotten very good at delivering that information back. We're not good at getting it to them, to be honest with you.

MS. MANNER: Erica, did you have a follow up?

MS. OLSEN: Yes. A quick follow up question though.

Several of the panelists mentioned as well the LMR Systems that are existing, that are out there, that are going to be there for a while. They say you want to hang onto your narrowband. What's the evolutionary path for that? Should we be repurposing LMR spectrum for broadband purposes such as the 700 megahertz narrowband spectrum?

MR. McEWEN: Not for the short-term because the technology isn't ready for that. I mean, somebody asked about LTE. I mean, LTE is in

development. It isn't yet ready for us. Some people are beginning to deploy some things but the next versions of it are what we're looking at for deployment.

MS. MANNER: Ralph?

MR. HALLER: Yeah. I guess I go back to pretty much a comment I made earlier that broadband 700 is not going to work everywhere. And I'll go back to in the forests. It simply doesn't work. You might as well turn the transmitter off because it doesn't penetrate through the trees and the pine needles. VHF does and it does very well. And that's why both the National Forest Service and the local and state forestry agencies continue to use VHF. They don't even like to go to UHF because it doesn't work as well in those areas.

It also takes a lot more infrastructure as Harlin pointed out just between VHF and 700. The amount of infrastructure is tremendously greater at 700 than it is at 150 megahertz.

Also, these sites that are out there --

because most of them were put in to public safety standards, they're already hardened well beyond what we're going to see in the commercial world for a long time. So, I think it's too early to begin to say let's go to a broadband solution for all of public safety. It's not there and it's not going to be there for a long time.

MS. MANNER: Thank you. I'm going to take one more question from the government panelists and then I'm going to open it up to the floor.

John Leibovitz?

MR. LEIBOVITZ: I guess I would just like to ask, you know, if you look over the last 10 years or more, you know, and you look at the way -- the sort of discussion about public safety communications evolved. It's evolved from, you know, there's been a lot of discussion about interoperable voice communications, especially in the wake of major disasters and then it's evolved now to broadband and we're talking about broadband. I guess in the context of that and

where we sit today, I would ask the panelists what do you see as the sort of single biggest problem in public safety communications today that needs to be solved for police, for firefighters, for other first responders? You know, if you had to pick one, what's the problem in terms of end-user capability?

MS. MANNER: John, if it's okay what I want to do is maybe poll the panel for that.

MR. LEIBOVITZ: Sure.

MS. MANNER: So maybe we can start with Charles.

MR. BRENNAN: I'm going to give you kind of an odd answer. We've run into it in Pennsylvania. We're able to connect networks fairly easily. We're operating on 800 megahertz. We can connect anything to anything; we've not failed. We've connected to disparate 800 megahertz system, VHF, UHF, low band. Everything we've connected to. Our hardest thing, believe it or not, is to figure out how we get all the people to actually talk once we connect them. And we're

actually working with it now. It has proven to be a much more difficult problem than the technical side of the equation. Everybody uses all -- I mean, okay, we're supposed to all use plain English but everyone forgets that they have their own jargon and they use their own department jargon which means something to them doesn't mean something to someone else.

When you connect people together, how do you know who you're talking to on the other end? Who is he or she? What is their rank? What is their authority? And it's been a monumental issue for us. The connection part has really been a piece of cake. It's that other part that we're trying to beat. We have like 1,200 public safety -- police departments in Pennsylvania; 2,500 fire departments. God knows how many EMS agencies. Trying to connect them all together and figure out when someone gets on one end of the radio talking to someone on the other end of the radio who is not in their department, how do you do that? It hasn't been easy for us to solve. We still have

not solved it.

MS. MANNER: Stephen?

MR. CARTER: I'd say the biggest problem is fragmentation: Every state and local group having a slightly different system. And when I say that probably most of you immediately think, oh, he means interoperability. And that actually is a very true problem, but I mean it more in an economic sense. I come from an industry where we have learned that when you have a unified market -- a lot of people all asking for the same thing -- an amazing amount of money gets spent; an amazing amount of synergy between all the different things you're doing comes into play; and you get amazing new capability deployed. And that's very different than what happens when each different police department, each different state is making a decision for their few thousand users and you don't get the economy of scale to do some of these amazing new technologies.

MS. MANNER: Thank you. Pete?

MR. EGGIMANN: I think I would focus on

connecting the communication centers and focus on the backhaul. If we had a nationwide network that was capable of supporting all of these applications we talked about that converge backhaul, we could do a lot at the local level than to leverage or build upon that. But we need that nationwide network on the backside.

MS. MANNER: Thank you. Ralph?

MR. HALLER: I think I would boil it down to funding. You know, when we're talking about trying to get broadband to public safety, we're not only talking about getting broadband to large cities with "unlimited" funding to lots of rural fire departments that buy their equipment through bake sales. And we're never going to get broadband to those entities who need it just as badly. But we're never going to get it there unless we can figure out a way to fund not only large but small entities in public safety so that they all have access to this nationwide network that's being built.

MS. MANNER: Thank you. Glenn?

MR. KATZ: Yeah, excuse me, I think the fundamental issue, the largest one, is being able to have 100 percent availability for our public safety workers. That means being able to have broadband in an area where there is no other terrestrial forms of communication. And also in all areas where there are terrestrial forms of communication, that if that terrestrial forms of communication are down, there needs to be a viable backup network. I think that's really the fundamental issue here.

And just sort of one little anecdote or interesting aspect to this, one of the other questions addressed what are we going to do with these LMR systems, these sort of archaic LMR systems? Based on practical experience that I see in the field, those radios are here to stay forever. Those people, the people that are actually using these devices like these things, they don't like to carry BlackBerrys; they're not used to them. So we need to be able to have basic voice technology and LMR communications to be able

to network at 100 percent availability throughout.

That's sort of the way I look at it.

MS. MANNER: Thank you, Glenn. Harlin?

MR. McEWEN: I agree with Glenn. Voice systems. If you ask a question, what is the one thing -- I'd like to have two -- but the one thing are not what we're here about today, it is the voice communication systems that need to be updated and improved for both operability and interoperability. A lot is being done. A lot has happened.

There's lots of progress but we will never give up voice communications, and I don't believe that broadband is yet -- you know, in my vision, in my lifetime -- is certainly not going to be the replacement for that. Broadband is secondary but is becoming increasingly important and that's why we're focusing on that.

MS. MANNER: Thank you. Finally, Bill?

MR. SCHRIER: I guess I lost track of the question. I was going to say video. High quality video. And if you get a device like this

that can send and receive video or images, that I think would be the most useful thing for public safety responders.

MS. MANNER: Okay. Thank you. I'm going to open the floor to questions. I actually have a few that have come in via the web. So I'll ask one of those to start. And then is Sue in the room? So we'll look for folks who have questions. But let me ask this one first.

There was a question from Craig -- and I apologize if I mispronounce anyone's name -- Chatterton on saying satellite communications are susceptible to weather situations, such as heavy storms and sunspots. How can such a network provide the requisite reliability? I'm assuming that Glenn would answer that.

MR. KATZ: Harlin, would you like to take that?

MR. McEWEN: No.

MR. KATZ: Sure, actually, yes, that is true but there are new technologies that are available today. New forms of modulation

techniques. Adaptability on modulation techniques that increase what's called the dynamic range of any kind of satellite system from where it was fixed years ago to being dynamic in 20 to 30 DBS, depending on the weather conditions. So I think we've made great -- the satellite industry has made great strides in being able to overcome what was some limitations when there are weather-related events for the higher frequency satellites.

MS. MANNER: Thank you. And let me ask one more from the web before we turn it to get whoever wants it on the floor. But this is from Kevin Haney to all panelists but whoever wants to answer it, please let me know.

How does broadband access help EMS in rural areas? Is there anyone who would --

MR. McEWEN: Well, it helps EMS. It doesn't matter whether you're in a rural area or not, but obviously in a rural area probably the biggest advantage is that they may be able to transmit and receive information from remote

hospitals where they can provide emergency care until they can reach a primary care facility.

MS. MANNER: Thank you. Laurie, did you want to add something?

MS. FLAHERTY: Yes. If I might, we're involved in a project with CDC where we are determining the specific data elements in Automatic Crash Notification that have the highest probability of predicting serious injury, and that will help rural EMS not only to use their sparse resource more efficiently but know where to take them. And also know where the location of the crash is which very often is a problem for them. That's just one example.

MS. MANNER: Thank you. And Pete?

MR. EGGIMANN: Yes, just quickly, just to build on what Laurie just said. If the 911 centers are equipped and are able to receive the information from the telematics people, we would be able to tell the ER how many people were in the car, whether they were belted in, how fast it crashed, all of that kind of stuff. Or even

better yet, we would be able to send that data directly to the ER so we wouldn't have to repeat it. But from the dispatch side of the coin, particularly in a rural area, it makes a big difference if I know I have to send two rescue squads because I've got four people in that car or I've got eight people in two cars or something like that. To be able to know right up front that I need lots of resources at that scene is a life and death kind of a thing. It can really make a difference.

MS. MANNER: Thank you. Do we have any questions from the floor? Sue has the microphone. So if you can identify yourself.

MR. DEVINE: Thank you. Steve Devine. I'm the interoperability program manager with the Missouri Department of Public Safety.

Two quick things with regards to the states and grants. The PSIC grants specifically allowed states to enter into MOUs with regions. And in Missouri, specifically, we built a statewide interoperability program and got, in

writing, memorandums of understanding from the regional -- the counties that make up the regions in the state to turn around and take the money. Also, the state provided the match which was favorable to the locals, and subsequently, turned around and offered that interoperable product to them.

So there is a way to actually go out and support and retain that money at the state level, but it does require an education with those regions and the counties specifically to retain those dollars.

With regard to data, I think before we get to a nationwide public safety broadband network, we're going to go to a nationwide public safety data network as was spoken. There are many places that don't have any data today, so I think this is an incremental thing. Everyone of us in this room at one point or another and our computers at home thought that dial-up at 56K was sufficient and none of us do anymore. So this isn't just one leap. This is something we're

going to get to as an incremental process.

Thank you.

MS. MANNER: Anyone else on the floor? Okay, I'm going to go back to our government participants. Do they have any more questions? Jeff?

MR. GOLDTHORP: A question about Next Generation 911 deployment, and I'll address it maybe first to Pete and then to the panel at large if they've got comments as well.

What strikes me about NG 911 is the bootstrapping issue. You know, how do you get started? There is a tremendous amount of moving parts to the problem, like lots of big problems. There's sort of a national service being deployed and, you know, there's standards issues; there's technology availability issues; there's deployment issues; there's, you know, integration with legacy technologies, existing technologies and networks. So, I'm wondering if there are case studies out there that folks are aware of where this has been bootstrapped successfully -- and we've got some

Next Generation 911 networks in operation -- and what the experience has been on that.

MR. EGGIMANN: Well, there's certainly projects underway. You know, Vermont, for instance, has a statewide system that is IP-based. There's a lot of talk about Next Generation systems being out there. The actual specs and the standards for NextGen aren't all complete yet so you have to take that with a grain of salt. There's some work being done down in Texas in regard to some of the Next Generation work.

The DOT project was certainly very helpful in that regard. We have a private project in the Minneapolis/St.

Paul area that we're just getting started with that's going to actually look at the processes in Next Generation all the way from when a customer signs up for service through the location determination, the routing, how the call arrives at the 911 center, the information that comes with it, and then on out to how do we deliver or disseminate that information onto

responders or to affiliated agencies.

So we're getting started but, I mean, the biggest lesson that we learned is that we need the IP connectivity. We need that wide area network in place. We know it's going to run on an IP network. And we concluded early on that it doesn't scale at an individual PSAP level. It has to be done at regional levels. You have to bring groups of PSAPs together.

MR. BRENNAN: Part of my last life was running the Philadelphia 911 center. A pretty big center; fifth largest in the United States. I can tell you we were on data overload already. Forget Next Generation. We were on data overload on this generation. And I think they're going to struggle, especially the big centers. We handled 3.3 million calls a year. We would handle between 10,000 and 15,000 calls on a busy summer day. And when I say handle I mean, you know, no matter how many people we put on the phones we couldn't even handle all the calls on some of the days.

Any technology that throws more data at

the 911 centers and then wants them to throw that data back out is going to be a big, big struggle for these big centers. You know, many of them are funded by surcharges on the telephones. That's not enough to run them. I mean, our center ran--maybe it paid for 40 percent of the cost, 50 percent of the cost. The rest was borne by the city. And to build new 911 centers--I mean, some people have done it; consolidated 911 centers--the cost is horrendous in these days and age. So I see it being an extremely slow process, especially for the big centers.

I've seen some smaller centers that, you know, really don't have a lot to do. I've been in a lot of them. They'll be fine, but they won't have the money. The big centers may have the money, but they can't handle -- even if they had the money they couldn't handle all the data coming in. They just couldn't.

MS. MANNER: Thank you, Charles. We have a question from the webinar from Doug McGillivray. I'm sorry if I mispronounced it.

But has there been any investigation to the ultimate cost of any of these proposals that are being discussed here today?

So I wanted to throw that out. If anyone has an answer -- everyone talked about a little different things. Bill talked about the fiber builds, some of the 911 issues.

MR. McEWEN: Well, I know in Seattle, Seattle has got about 320,000 premises, homes and businesses, apartments and condos. It would be half a billion dollars to connect everyone of those with fiber. We've got a fairly firm estimate on that. Now, half a billion dollars for a city of 600,000 sounds like a lot of money until you consider that we're going to spend $4 billion, 8 times as much, to replace a single freeway on our waterfront divide up. So for one-eighth of the cost of replacing a freeway that carries 100,000 vehicles a day, you can put fiber optic cable to every home and business in a major city.

MS. MANNER: Any other? Okay. I have one question and then I'll call on Kathryn.

This one is not for attribution, but when I drove here if an emergency vehicle was behind me I got out of the way. Why did we not hear one mention of modifying the 3496 axed for priority access? Is anyone able to answer that?

Okay, we'll put that aside. Kathryn?

MS. MEDLEY: Thank you. I noticed a lot of focus on the terrestrial infrastructure and the fact that there's not a lot of bandwidth available via the terrestrial means at this point.

There is a goodly amount of bandwidth available in the sky via satellite, and I was wondering why public safety officials aren't looking at that particular aspect to help with some of their data requirements today and in the future.

MR. McEWEN: Well, I think we are. We're certainly looking at satellite as an option. Unfortunately -- and Glenn may take me to task on this -- but, unfortunately, the latency of satellite for public safety is getting better but it hasn't been, you know, to the level that we

need for every day kinds of use. So, we look at satellite as an important aspect of this to mix with terrestrial, but mainly as a backup for terrestrial when it isn't available. And secondly, for filling in where there isn't ever going to be any terrestrial.

MS. MANNER: Anyone else? Charles?

MR. BRENNAN: We're now running a large LMR. It covers 45,000 square miles. And we've experimented with satellite with great success. The latency wasn't bad. We kind of thought it would be but it was very tolerable. And we eventually will integrate satellite, you know, into the network. I think it's a combination of a COW when you can use it, a satellite when you can't and, you know, LMR when that's what you have. It's going to be a combination of all three.

I think what scared us the most about this -- as you talked to the different providers it was sort of like buying a car. You know, you weren't sure about the rate plans. You know, the

rate plans got a little complicated. I'd like to see them much simplified and I think that kind of scared us off a little bit. Technology seems to have dropped in price. Even the rates seem to have dropped in price. And I think the satellite provider has got to be a little more aggressive in coming to the show, simplifying their rate plans, because public safety tends to be a little skeptical anyway when they buy things. So I think the simpler the better.

MS. MANNER: Thank you. Any other -- oh, do you want to add something, Ralph?

MR. HALLER: Yes. I think it also has to do with the number of handsets you have to carry. One of the problems in the past, even on the land mobile systems is to get interoperability a fireman or a policeman has to carry three or four different radios because they're all operating on different frequencies and, you know, it's continually juggling between those. You add broadband to that and then you add satellite on top of that and now we've got another couple of

radios that they have to deal with. And so part of what is going to make this all come together, I think, is probably the software defined radio that allows communications in any of these modes rather seamlessly as opposed to having to do it on different pieces of equipment.

MS. MANNER: Actually, I have a question. I'm going to follow up on what you said and ask Stephen. On chipset technology, do you see the current chipset technology able to address some of these issues of having multiple radios?

MR. CARTER: Certainly. Already the latest cell phones that come out now support pretty much worldwide operation and that's just because it's become so much less expensive to put everything into the chips than it is to do different chips for different parts of the world. And, in fact, we've been working with some of the satellite providers in the United States, the ATC companies, to put a satellite mode in future generation chipsets. And those will be coming out in about the next year.

So, it's entirely possible that you will see handsets, cellular handsets in the near future that will have a satellite mode, also. But that march onward continues. And certainly the policy issues of interoperability won't be solved as easily, but the technology issues I think will be.

MS. MANNER: Thank you. Any other questions? Go ahead, Charles.

MR. BRENNAN: This one probably can be more for Mr. Haller and Mr. McEwen.

One of the issues that we're trying to avoid in FEMA is doing exactly what you said, Mr. Haller, and that's putting a bunch of radios in the first responder hands. We're trying to fit more into the local environment when we get in now via the various patching equipment that we have: Audio patching capabilities, network gateways, and such. But a lot of efforts have been going into now into shared systems, and the federal agencies are moving into these shared agreements based on MOUs and a handshake.

Being we're at the crawling stages right

now on the broadband side, regardless of what spectrum band we're looking at -- this is more of a food for thought thing than a point of debate -- but I think federal agencies would probably be a little bit more apt to invest millions of dollars into a system where they co-primary or of equal access to a broadband system other than on some of these sharing agreements they may in the future, based on requirements, be kicked off the network after investing millions of dollars to be on a sharing situation.

Any comments on that?

MR. HALLER: I think this has been a problem for as far back as I go in this which is almost as far as Harlin. It's been a problem getting sharing of resources between federal, local, and state governments for a long time. I used to say that the federal -- no offense -- the federal government's idea of sharing with a public safety entity was "let us on your system." In other words, very little the other direction. And I think this is changing. The federal government,

I think, is working much closer with trying to integrate systems that are there for FEMA and other agencies with complex systems that are in place for state and local agencies.

So, I think this is going to improve with time and with trust. But honestly, there's a history of years and years and years and years and years of mistrust that we have to overcome before that's going to become as smooth as we would like it.

MS. MANNER: Harlin?

MR. McEWEN: Yeah. I think Ralph is correct, but in the broadband vision that we have at the Public Safety Spectrum Trust, the vision is a different vision than the past. In other words, it is not necessarily to have the federal agencies as co-primary, but certainly as a full participant in some way. We haven't figured out exactly what that means. In the second report and order it gave us, the public safety broadband licensee, the responsibility for coming up with a way to do that. And our vision is that federal agencies

have to be a primary user of the system. How that works out and what kind of sharing, I'm not quite sure yet. It's an unknown. In fact, I'm meeting with some of the government CIOs tomorrow to talk about some of those issues. But we clearly have a vision that the federal agencies have to be a big user of this system.

MS. MANNER: Thank you, Harlin. We have one question from the webinar from Scott Andrews who asks as a panel, what do you feel the role of the local planning committees may be, if any, as we move forward into 700 megahertz broadband?

Is there anyone who wants to -- okay, we'll skip that. John?

MR. HALLER: Is that talking regional planning committees?

MS. MANNER: Yes.

MR. HALLER: Harlin?

MR. McEWEN: I wasn't really paying attention to the question.

MS. MANNER: I can repeat it. What do you feel the role of local regional planning

committees may be, if any, as we move forward into 700 megahertz broadband?

MR. McEWEN: Where they exist -- and, in many cases, they do exist and are very active -- we believe they have to have a big role. Unfortunately, they're not all equal. Some are better organized than others and in some places they don't exist. So we have to have a mechanism to make sure that this nationwide network is delivered equally to all users. But I believe that they will -- where they exist and they are well organized they should be a part of this effort.

MS. MANNER: Thank you. I have time for one more question. Oh, Ralph wanted to add something.

MR. HALLER: I'd just also say that right now, at least from a regulatory standpoint, the regional planning committees don't have any specific involvement in broadband.

To the extent that they work with the public safety broadband licensee voluntarily,

that's great, but they have no specific obligation under the FCC rules right now to be involved with broadband. So, I guess what I'm trying to say is they don't really have a role but their help is welcome.

MR. MANNER: Thank you, Ralph. John Leibovitz for our last question.

MR. LEIBOVITZ: My question is about we talked about the how and the what. So the what is broadband; the how, different mechanisms for bringing it. I want to just talk a little bit about the who -- who uses this network and who we see as the users initially as it rolls out.

So I guess my question is, you know, do you initially see, when you think about public safety broadband networks, the initial users are -- take the fire scenario. The firefighters in the building, you know, or are they the incident commanders, you know, communicating over some other media such as LMR systems or some other system to the responders inside the mission critical situation? How do you see the sort of

use case evolving and for who needs to use the system first and then over time?

MR. HALLER: Well, in the beginning I don't believe that this will be a primary mission critical-type system. I go back to the fact that voice is going to be the critical thing. Two Buffalo firefighters just died, I think, yesterday in a tragedy and luckily they were able to get word out that the one first of all was trapped and saw him. But the fact is that I don't believe firefighters in a burning building are going to be using a text device or a data device. It's going to be different than that. If they had that device and voice capability is existing and one of their voice radios isn't working that may be their lifeline.

So, but I think, you know, the primary users are going to be the police, fire, and EMS, the first responders.

They're going to be the primary users. Then you're going to see what I call the secondary users -- utilities, transportation -- other people

that often are there very quickly that need to be a part of that.

MS. MANNER: Bill Schrier?

MR. SCHRIER: The users of -- remember, this is a National Broadband Plan. The users of this will be every person who lives in the United States of America or works in the United States of America, because they're the people who call 911. It's their safety that we're trying to protect. It's their -- it's those people that the police officers, the firefighters, the EMS serve. And ultimately, a National Broadband Plan has to connect the people of the United States to their governments and to the agencies that are keeping them safe.

MS. MANNER: Thank you, Bill. And I'm going to let -- actually, Charles is going -- I have to cut us off. Charles is going to have the last word since he was the first one.

MR. BRENNAN: Great. I think you'll see it deployed in three stages. First, broadband to the 911 centers. And the 911 center dispatcher

would translate what he or she sees on the broadband screen out over voice to the field. Second stage would be wireless to the command post, where the command post is now closer to the scene of the incident has access to broadband, whether it's video, data source. And third is right to the final user, to the end cop or end firefighter in the field. I think you'll see it in those three stages.

MS. MANNER: Thank you so much. What I would like to do is first thank all of our panelists and our government participants and the folks online and in the room who asked questions. But I'm going to ask you all to stay seated right now because we just have some brief comments from Dan Phythyon and from Charles Hoffman. And then we'll take a 10 minute break.

So with that I'm going to turn the floor over to Dan. Dan, you can use either the dais or from the table, wherever you prefer.

MR. PHYTHYON: Yeah, I think I'm on the five minute clock so I'll stay here if that's

convenient.

First, thank you very much for inviting me to participate on behalf of our office. This is the FCC's work, its task, I guess, in developing a National Broadband Plan is incredible. The effort you're putting into this this month and beyond this month is enormous, so I feel your pain. And we're happy to participate and to also share from what the information you're uncovering.

Very briefly, what is the Office of Emergency Communication? Our director a number of months ago did a bigger briefing on the office at the FCC at one of the workshops so I won't cover all that, but in short, our office is part of the post-Katrina reorganization of DHS that Congress enacted. And it was in response to Katrina demonstrating once again that we still haven't figured out emergency communications -- how to make it work, how to make it -- interoperability work consistently. So, our office, we are not operational. We don't deploy, as our colleagues

at FEMA, Charlie Hoffman's shop, does.

Our office is primarily a policy and strategic office. And one of our tasks from Congress was to, for the first time, develop a national emergency communications plan at a strategic level to try and knit everything together. That plan was delivered to Congress about a year ago. And by design that plan really was focused on some of the legacy issues with land mobile radio communications, some of the things that Harlin alluded to which we still haven't figured out. That part of it and much less the future. And the roadmap to the broadband technologies we're talking about today.

So we essentially focused on, again, legacy issues and legacy solutions, and a lot of what we focused on really isn't the technology. We heard again today something we hear very frequently, which is that technology, as difficult as it can be, it's the easiest part of making it work. What is the rest of what you need to do to make emergency communications work? It's the

people stuff; the softer stuff; the governance; standard operating procedures; training and exercises; usage issues; funding issues. So those are the things that we focused on in that first generation of the plan and we said we'd get to the rest of it later.

Well, earlier this month our secretary told us, okay, later is now. You guys need to work on upgrading that plan, taking it to the next generation, and dealing with some of the key broadband issues that are the subject of the FCC's task and the work we're talking about today. So we are going to be working -- collaborating very closely with our federal colleagues, state, local, you know, tribal entities--the same way we worked collaboratively to develop the first generation of the plan. We're going to embark on building in new elements of the plan. Seven hundred megahertz issues. Broadband issues more globally. The Next Generation 911 issues that DOT and the FCC and working on and Nina's working on. Alerts and warnings. Those are things that we're going to be

working to embed into the next generation of the plan.

So, again, we've enjoyed the collaboration we've had, in particular with the FCC to date. We're going to continue to collaborate furiously with the FCC. I'm looking at Jeff Cohen here in the front row. We're on each other's speed dials. We probably get sick of talking to each other multiple times of the day and many weeks, but we're going to continue to do that. We're going to work closely with the FCC on the public safety aspects of the National Broadband Plan, and we are going to borrow enthusiastically from that and put that into our own work.

So, again, thanks for the opportunity. I appreciate all the hard work that you're doing. I think my sense in sort of wrapping up my comments is probably the same of a lot of you. We have barely scratched the surface today of these issues and look forward to a lot more work to figure out, you know, how to make the National

Broadband Plan work for our emergency responders and ultimately the public we've talked about.

A couple of concluding points. There's already been a lot of discussion today about funding issues. Public safety conversations of this sort, no matter where they start off, they always end up with funding. That's going to be a key issue. We've talked about grants. We've talked about other options, whether it's universal service issues, tax issues, tax credits, but please, as we move forward, think about funding issues. And we've also talked -- Ralph mentioned earlier some of the sharing issues. Part of our office's mission is to, again, break down some of those barriers, improving sharing of all types between federal and nonfederal entities and across federal entities so that we're looking forward to that being, again, part of the solution to broadband is to think more creatively about -- we have the opportunity as we build in the new broadband infrastructure to share in ways we haven't before, including with the private sector.

So, thanks. And I look forward again to a lot more work by all of us.

MS. MANNER: Thank you. And you finished right on time.

And with that I'd like to turn it over to Charlie Hoffman from FEMA.

MR. HOFFMAN: Thank you very much, Jennifer. And thank you to the Commission for inviting me over to participate in this panel today. It's been a very eye- opening, enlightening experience sitting in on this.

Going along with what my partner Mr. Phythyon said over in the Office of Emergency Communications, we work hand- in-hand with them in the Emergency Communications side of the National Emergency Communications Plan. We've also formed a great partnership with the Commission on providing emergency communications spectrum analysis when we get in prior to an incident -- a planned incident, such as a hurricane or a national security event -- and then post-incident where we can go back in. And we've worked out a

very good agreement with the Commission on that. And we look forward to our continued working with the Commission on emergency communications response.

Part of the Disaster Emergency Communications Division -- we're a spawn off of the post-Katrina Emergency Management Reform Act -- and learning from the lessons from Katrina, one of the words that you hear a lot for public safety grade communications is survivable. If all communications systems were survivable, we'd be out of business at FEMA and Disaster Emergency Communications. As we found out during Katrina that not only was interoperability not there, we did not have operability. For whatever reason. The public safety systems themselves, the repeaters or base stations may have been fine, but the generators got flooded out which now prevented the repeaters from operating.

Part of FEMA's job to come in when we respond in a disaster is to provide a federal response coordination on communications efforts.

That's part of our job when we get into a Type 1 or Type 2 major incident, be it manmade, be it a natural disaster.

Part of our -- one of our major units within the Disaster Emergency Communications are our Mobile Emergency Response Support Units. We have six detachments based throughout the United States. Five of those 6 detachments support two of our FEMA regions -- 2 of the 10 FEMA regions -- so that they are within a 500-mile response capability for any type of disaster -- major incident, manmade -- whatever that may happen. In our MERS units we have various amounts of mobile disaster response command and control operations center vehicles. These vehicles provide a rapidly-deployable multimedia interoperable communications systems for the incident area.

Of our primary vehicles that we use was what we call the incident response vehicle, the IRV. That vehicle is capable of doing pretty much almost DC to daylight-type communications. We can do audio-based band switching for LMR. We can do

gateway interfaces. We can do satellite backhaul capabilities. They also have the capability of extending out the network as we have tested in some of our capabilities of 500 to 700 yards around the vehicle using Hotspot/WiMAX/WiFi-type technology where we can bring operational tents, centers, around the IRVs and they can have seamless connectivity back into the networks that we backhaul via Ku band satellite-type equipment.

We're in the process of upgrading all of our mini emergency operations vehicles, which is a little bit larger vehicle than the IRV, but up until now, they were pretty much just a mobile command and control vehicle that had external Ku band capabilities that proved kind of hard to do so we started installing their own Ku band satellite backhaul capabilities in there to provide Internet and voice communications backhaul capabilities. We are now going to expand those by putting in Cisco routers, WiMAX WiFi so that these new vans or the vehicle with their new capabilities will have the capabilities to

provide--extending the network out just like the IRVs do. And in fact, some will even have more capabilities as we're going to be expanding into secure voice teleconferencing, video teleconferencing, those capabilities. Streaming video has become very big for us after Katrina for bringing situational awareness back to headquarters and to our regional administrators. And as you all know, streaming video is a bandwidth -- huge bandwidth requirement.

I'm right down to the end of my time here, and once again I'd like to thank you for having me here today.

MS. MANNER: Thank you, Dan and Charlie, for sharing those comments with us. And once again, thank you to our panel.

(Recess)

MR. LANE: Good morning, ladies and gentlemen. Let us begin our second panel of today's broadband discussion.

My name is Bill Lane. By position I am chief engineer in Public Safety and Homeland

Security Bureau of the Commission, but more importantly, I have the pleasure of moderating our second panel today.

At the beginning of our second panel I'd like to mention that Commissioner Copps had intended to attend today's session but unfortunately his scheduling, as well as the scheduling of our other commissioners and the chairman, prevented his attendance in person. However, I do want to mention that all of the commissioners and their staffs, as well as other members of the staff of the Commission are viewing this via internal television, as well as the web presentations. And they are very closely following our proceedings. And so I can assure you that there is a high level of interest among the commissioners and their staffs with the proceedings today.

Our second panel will examine the ways in which broadband technology can enhance homeland security. The panel will explore how best to utilize broadband technologies to prepare for,

respond to, and recover from major natural disasters, pandemics, acts of terrorism, and cyber attacks. It will focus on how public safety networks and applications can be secure and protected. The panel will also examine current and potential new applications and research that has been conducted in the managed IP arena that could help improve response to the large-scale emergencies.

Our second panel consists of the following, and I'll provide just simply a brief introduction of our panelists. First, to my immediate left, Dr. Andrew Afflerbach, chief executive officer, director of engineering for Columbia Telecommunications Corporation and representing the National Association of Telecommunications Officers and Advisors.

Next to Mr. Afflerbach -- Dr. Afflerbach -- is Dr. Emmanuel Hooper, senior scholar and researcher, Harvard University, Leadership for Networked World; Harvard-MIT-Yale Cyber Scholar; and founder of Global Information Intelligence.

Next to him is Mr. Murad Raheem. Excuse me. Mr. Raheem is branch chief, the Office of the Assistant Secretary for Preparedness and Response; Information Technology, Electronics and Communications for the U.S. Department of Health and Human Services.

Adjacent to Mr. Raheem is Mr. Marc Sachs. He is executive director for National Security and Cyber Policy in the Office of Federal Government Relations for Verizon Government Affairs.

And our last panelist today is Mr. Steve Souder, director of the Fairfax, Virginia Department of Public Safety Communications.

And on a personal note I'd like to at this time also extend another time a public thanks on behalf of the Commission and the people of Virginia to Mr. Sauder. Mr. Sauder was the director of communications for Arlington County on 9-11 and directed the communications response to the county across the river at the Pentagon. So once again, Steve, thanks from all of us for your

great service.

Our government participants today are, first and foremost, Mr. Charles Hoffman. Once again, chief, Disaster Emergency Communications Programs for the Federal Emergency Management Agency; excuse me, Mr. Jeff Cohen, senior legal advisor for the Public Safety Homeland Security Bureau of the Federal Communications Commission; Mr. Jon Peha, chief technology officer for the Federal Communications Commission; and again, Mr. Dan Phythyon, chief, Policy, Planning and Analysis Division for the Office of Emergency Communications, Department of Homeland Security.

So please join me in welcoming our panelists and thanking them for coming today.

As we did in our previous panel, we'll begin with some prepared remarks from our panelists. Once again, I have command of the hook and will employ it vigorously as needed.

And so we'll ask our panelists each to open with five minute comments. We'll begin with Dr. Afflerbach.

DR. AFFLERBACH: Thank you. Today I'm speaking on behalf of NATOA and the National Association of Counties. What I'm bringing you today -- if you can bring up the next slide, please -- is models telling you that we have models that are supported by empirical data for how very distinct partnerships between carriers, cable companies, and localities can support fiber optic broadband deployment and public safety networking. So attending to both things at the same time. And we recommend that the FCC look to these models.

Franchise infrastructure, also known as I-Nets -- Institutional Networks -- are in our finding one of the most successful local government private-private partnerships in communications history. And what they are is essentially extra fiber optic capacity that were built by the cable operators and paid for by the localities at the incremental cost. It's an extraordinarily efficient way of building, in this case, two networks for the price of one. In this

model we realize significant efficiencies all on one platform; the ability to, at the direction and activity of the local government, build an authentic public safety grade platform within a cable company carrier infrastructure. And the Cable Act, as it was written, allows localities to negotiate I-Nets with cable companies. Well over 100 of them exist across the United States and these range from small localities to major metros, East Coast, West Coast, Midwest.

Next slide, please. Unfortunately, with statewide franchising and renewals of franchise agreements and a generally deteriorated sense of the local governments in negotiations, some of these networks are at risk. And that is something of real concern as we see it.

Next slide. The networks as they are built are varied from locality to locality but generally we're hitting every single major building and piece of infrastructure. We're going to locations where cameras and signals are needed. We are hooking up backhaul for public safety

communications, whether it's LMR or broadband. We're going to the police stations, going to the fire stations. The applications that operate on the network are everything from the interactive video discussed earlier; dispatching information, which as we know has become more graphics intensive. We've got the need to push building maps and plans to the first responder stations.

We've net patient tracking. We've got backup of emergency operation centers in real-time. We have in short many critical high bandwidth applications that are going live on these networks.

Next slide. 9-11. New York City had a fiber optic network in place in partnership with the cable operators there. This was the only network in that part of Manhattan that stayed live. It was a SONET ring. It was built to the specification of the local government of New York City and it continued operating and was even used by the carriers to restore communication.

Next slide. This was recognized by the

Congressional Delegation so that when national franchising, which would have jeopardized this network was on the radar -- next slide -- essentially the Congressional Delegation and others went to bat to keep this network and the national franchising did not pass.

Next slide. Essentially, what we're addressing here are the drawbacks of traditional off-the-shelf lease-carrier services, the fact that the architecture is not, in most cases, transparent and in many cases proprietary and not visible to the locality, to the fact that maintenance and architecture is driven by broader business considerations, not the survivability that's necessarily needed. We've got shared infrastructure that may jeopardize capacity in critical conditions. And we have issues of power, as well.

Next slide. And this you can look at at your leisure later on but there are also issues as far as provisioning and single points of failure that can be addressed.

Next slide. Washington, D.C., is an example of a network where ring architecture was used throughout, and right now FEMA is connected through this network. There was activity going on to potentially offer this to federal government to address some of their needs.

Next slide. Ten to 20 times is essentially the cost of what it would be to essentially replace these services with comparable market price networks, so we're talking about a few million dollar tax increase essentially for the citizens of a medium-size county to replace these services if they're lost.

Next slide. More affluent communities see that in the long term it' beneficial enough to build a network but this is only an option for the more wealthy communities.

Next slide. So, essentially we're saying -- we're not calling for building a whole new infrastructure, spending billions of dollars. We're calling for the localities to be able to keep what they have in terms of functionality and

in terms of cost structure.

And I thank you for allowing me to speak on this subject.

MR. LANE: Right down to the second. Congratulations.

Our next panelist is Dr. Emmanuel Hooper. Dr. Hooper, please.

DR. HOOPER: Thank you. This is a very interesting topic, as a matter of fact. The 21st century intelligence, this country and around the world faces tremendous challenges because broadband security brings us into a new kind of phase of challenge for security.

High-speed networks, look at the next slide, please. We have intelligence issues to consider. One of them is basically how do we deal with facing broadband and cyber networks with high-speed acceleration of broadband networks via wireless, WiFi, emerging WiMAX to cyber infrastructures. Some challenges of high-speed transmission requires high bit data transfer -- gigabits, and eventually terabytes -- across data

networks across the world, including wireless and fiber networks that interconnect the global network and Internet. So, when we come to broadband distribution we have issues of access control, security monitoring, increasing detection, prevention, and forensics evidence, as well as traceability, and also sustainability of use of management.

Next slide, please. So we come to the aspect of this broadband plan to address how to protect advanced cyber security. The broadband plan for Congress surely should include strategic ongoing research because on a wider impact, we have to understand what broadband opportunities will give to both hackers as well as those who have a very good understanding of how astute workers can work. That is, to ensure that there is a way to intercept high-speed traffic of various segments of broadband infrastructure that interface with U.S. Cyber and global networks that transmit high-speed data in real-time. We have to identify the difference between legitimate

traffic versus traffic at different levels, different traffic providers -- I actually don't understand this -- and look at effective key management in terms of cryptographic key management, ciphers, algorithms, and adaptability to handle astute interceptions, evasions, and insertions.

Next slide, please. Strategic ongoing research describes how we understand what is actually happening. When it comes to FCC coordination with other federal agencies and state and local governments, we need to understand how to differentiate between coordinated research, intelligence on broadband, and cyber security for FCC, Cyber Coordination Executive, and National Cyber Study Groups, such as NCSG, and the DNI, as well as FCC regulations, and DHS, et cetera. Or call DOD, and DARPA, and IARPA, et cetera. All of these can actually coordinate together. The intelligence should be gathered together with effective coordination with state and public national security, as well as at local levels for

government agencies for large-scale events. This involves the importance of developing effective management standards; research, development of distributive broadband networks; and strategic, what I call intelligent hybrid data mining for broadband networks.

This is still ahead. So many times some companies -- one of the companies I work for -- other companies such as Open Sky, et cetera, and some of my students often discuss this. How do--

The next slide, please. We talk about the 21st century. How do we deal with mining interception, what we call intelligent understanding of our enemies or counterintelligence.

A speaker from DNI was talking to us at MIT and Harvard. The question is -- and I taught a lecture and one student asked me what is counterintelligence and who is our enemy? The question is what is the capability of the "man-in-the-middle" to intercept data and traffic at high speeds?

When you come from wireless and go out to private networks that actually come to you as data intelligence, because most of the traffic that comes from student hackers comes from the private networks which the intelligence community cannot really have access to monitor that. So we need real-time data traffic and hybrid networks -- what we call intelligent -- astute adaptable intelligent algorithms. And then, of course, in real-time you can scale these. I've done some research. You'll see my reports later on.

Next slide, please. These algorithms, what we talk about is intelligent hybrid techniques, the friendship between what has happened on the global networks and in the private networks and to the public networks -- they cannot really look at the traffic in real-time. So the local and regional -- we cannot get data; we can intercept data; we can pass the data; and of course, we can analyze the traffic. And in real-time, we recommend that Congress actually puts in not just funding but strategic research

measures so that you can actually see the impact of it long term.

Next slide, please. So, we come to the analysis here. We look at how do we analyze -- we need to actually look at large-scale events and what we're going to do for the 21st century. Cyber security for the United States, actually, we're behind in terms of the 20th century. If you talk to the White House and the Security Council Group and other groups, as well as DNI, we know that we don't understand really -- we're not really looking at what we call meta data transfer from virtual private networks around the world at different data centers, but terabytes per second -- over 25 terabytes per second at each data center. And then we're looking at stealth attacks and many types of analysis.

Next slide, please. I have a paper online, but this is very important to understand how to engage researchers -- the FCC should do this on clear data mining, broadband as well as other strategic measures and look at real attacks.

My final slide looks at references, and you can go on the slide and get more data.

Thank you.

MR. LANE: Dr. Hooper, thank you very much, indeed.

Our next panelist is Mr. Murad Raheem from the Health and Human Services perspective.

MR. RAHEEM: Good morning, guys, and thank you, Bill and all the folks at the Commission for having us here.

Next slide, please. Basically, very generically, why is HHS here and why are we interested in public safety and broadband communications? HHS as a whole is a very large agency. As you can see, a $707 billion budget, about 65,000 employees, mostly doing public health research: FDA, CDC, things of that nature, NIH. The part that I am involved with is the actual emergency response. So, the Commissioned Corps is a public health service and --

Next slide, please. What brings us to bear was the Pandemic and All Hazards Preparedness

Act in 2006 bringing the National Disaster Medical System back to HHS. It was originally with HHS when it started, moved to FEMA, and then came back to HHS in 2006.

They are actually our first responders -- or we like to say second responders -- who work for a public health emergency to augment state and local folks. When we go out in the field, we do a lot of things that require broadband access very loosely defined. We do a lot of voice communications.

Next slide, please. Our mission, obviously, leading the nation, preventing, and responding to emergencies. And the vision obviously is to hope that the nation is prepared. The more the nation is prepared the less we have to do, and that is certainly better for all of us.

Next slide, please. NDMS, specifically, is our partnership with the VA, FEMA, and DOD -- about 9,000 -- 8,000 to 9,000 intermittent federal employees. But these are folks that are normal, everyday healthcare providers in the normal work

life. So they're respiratory therapists, docs, EMTs, et cetera. We bring them together as a 35-member team to respond and assist local or national disasters. Right now it's mostly voice communications with some limited data for electronic medical records. More and more we're seeing that's an area where we can use broadband. And if that broadband is in the area we're at or if we can, as someone said brilliantly earlier, drag it to where we are, we can use things like prescription data records to know that the folks that are presenting to us need diabetic medications and what those are.

So, we really see us as a customer for broadband networks. And we lean very heavily on FEMA and Charlie's folks, especially in the MERS world, to bring us many of those communications. All of our walkie-talkies are programmed by the MERS guys to ensure interoperability. But more and more we're seeing the need to do this broadband communications.

Next slide, please. Our sector's

operation center is a 24-by-7 ops center -- that's down the street here--and more and more they want to know what's happening in the field. And things like video, which we hear a lot about, patient data, who is presenting--especially in areas such as pandemic influenza during, say, a hurricane event. Say we're doing a hurricane in -- we saw Hurricane Bill a couple of weeks ago, dealing with the folks that present for hurricane injuries, but may have influenza-like illnesses. And how do we deal with those in a normal scenario where we put a bunch of people in a very small space? Now we have to maybe spread those folks around and obviously, broadband gives us more ability to have more people do more things.

Next slide, please. We bring a mobile command post to bear. And this is 2001 technology built after 9-11. There's a satellite dish in the back, but it's got 128K and it doesn't work for most of what we need. So we bring and augment it with Ku satellites. Again, go beg, plead, and steal from MERS to borrow stuff.

Next slide, please. So one of the things we want to get out of this panel if at all possible is how do we ensure that sufficient reliability and redundancy of the broadband communications infrastructure is there? And what we really see is the sort of mobile solutions. We roll into a gymnasium or the Superdome, things of that nature, where there may be inherent technology there but we can't use it. It's proprietary. It's the hotel; it's the motel; it's the whomever.

Electronic medical records, obviously, is the next big thing for us and we're using them now. Obviously, how can the feds help? Clearly, funding. We've seen that and heard that a thousand times. Our hospital preparedness folks grant about $300 million a year to that effect. And national standards. Our office of -- the National Coordinator for Health IT is doing things like Project Connect, which has a VPN-like solution for healthcare providers to connect via the Internet, basically, and let the folks that

build the networks better than we do build the networks. And if we could do -- if we could sort of jump on them and abuse them, that's what we'd like to see.

Thank you.

MR. LANE: Excuse me. Mr. Raheem, thank you very much.

We now turn to the commercial sector and to Mr. Marc Sachs from Verizon, please.

MR. SACHS: Thank you, Bill, and other members of the Commission.

I guess it would be if you build it, they will come. That's the way we wrap up.

I am of a security mind --

MR. LANE: And you are building it.

MR. SACHS: And we are building it. I am of a security mindset. Around my office a lot of people don't like it when I come in because it's usually I'm bearing bad news about some new threat or something evil or something that's about to break.

What I'd like to spend a few minutes

talking about is this world of cyber security and how it intersects with broadband and the growing threats that are out there and the ways that we can counter this. And also offer that while security is not 100 percent -- we can't always do that -- we can make it part of the rollout. It's like a good haircut. We could just make it sit there. We don't see it, we don't know it's there, but it's in place and it does what it's supposed to do.

Next slide, please. Just so we're all thinking the same thing, there's lots and lots and lots of cyber problems. They range from Internet fraud, which we're all very familiar with: The fishing sites, credit card theft, identity theft, things like that. We have a lot of malware. Malicious software. This is code; we don't even know we've downloaded it onto our computers. You visit a website; it injects something onto your machine. You don't even have to click "okay" anymore. It just automatically downloads it for you. It's very helpful. Some people call these

value-added features.

Broadband, of course, makes this a lot faster and a lot easier for the malicious types to inject that type of code into our systems. We've got different payloads from spyware to keystroke loggers that can monitor everything you type in. We've got Russian organized crime and Chinese and others that are taking advantage of this broad connectivity that we have. They conceal themselves quite well. They can hide completely within your computer with no knowledge that they're there.

Why do they do it? Well, it's very much like asking a bank robber why they robbed a bank. It's where the money is. That's where the goods are. And they will go after anything that's connected. It doesn't matter how fast or how slow it's connected. And they'll certainly go after those things that are connected faster because then they can download and extract from you more value faster, quicker, cheaper than they could before.

Next slide, please. So if we look at the future and where we're going with this, emerging threats -- as we get more, faster, creative-types of applications, we're going to have more, faster, and creative-types of threats -- people that want to do bad things. We've already seen social networking applications as the Facebooks and the Twitters of the world being attacked. We see Smart phones becoming a victim. Voice over IP. Other types of new technologies. We've got countries now that are targeting us. They would like very much to go after our public service networks. They'd like very much to attack our soft underbelly, and they will continue to do that.

Next slide, please. So, if you look at how our networks are built -- and there are countless diagrams that show networks. This is one of many oversimplifications but I like to show it because along the left side in the outer rim you see all the different types of users: Critical infrastructures, law enforcement, public

safety, and others, all connected to this nice little cloud where we have the word "convergence" in the middle. And you might notice from some of the acronyms there, these are different types of protocols, different types of networks, all coming together. And, in fact, six or eight years ago we thought we would have been converged by now. The rumor was that by 04-05 there would be just one network; we'd all be doing the same thing. But yet now in 2009 we look back and say, well, maybe not so fast. Maybe that convergence didn't work out the way we thought it would.

And, in fact, sometimes diversity is, in fact, better so that we have an alternative means if something collapses. If a bad guy gets in and breaks things we have a second way to go.

I do want to point out though that the Internet-- the little cloud in the upper right hand corner--is not necessarily directly connected with the public service community, or the first responders, or any others that are working in this community. A lot of times we have a very strong

gap between those two. We might even have managed IP networks that run the same protocols as the Internet but they're not connected to the Internet. All these, unfortunately, still are targeted though and many of our threats come through the Internet so we have to be careful about that interconnectivity. And anything that we do build, particularly in public safety, has to be separated from the Internet as best as we can or at least have some kind of strong safeguards there because that's where the bulk of the threats come from.

Next slide, please. If we look at the way industry has been responding, we've been trying very hard over the years to stay in front of the threat. Of course, this is a very complex problem so staying in front is hard. We've been able to mitigate a lot of spam. We're identifying viruses. Everybody has anti-virus software. Most of the major carriers have managed services now working directly with customers to help them manage their networks. We offer parents control.

We have education for kids. So certainly there is a leaning forward and a recognition of the threat.

Next slide, please. There is a big push to have Smart Networks, open networks, open protocols. There's a lot of opportunity to do this right. There's also a lot of opportunity to do it wrong. We can build Smart Networks that can detect malicious activity. They can heal themselves. They can see it coming.

They can fix themselves. We could also leverage the competitive nature of the open world and of companies that like to compete to fight this.

We need to look forward. Opportunities like the Smart Grid, Health IT, other places give us places where we can counter this growing threat and build new networks that are optimized for that.

Last slide, and we'll take this up in discussion. What do we do next? How do we look forward? And I'll offer that up as a Q&A as we move forward. Thank you, Bill.

MR. LANE: Very well. Thank you very much. And our last introductory comments this morning are from Mr. Souder. I might add that Mr. Souder not only was with Arlington County in the Pentagon on 9-11, but he subsequently has worked in Montgomery County in Maryland, and now, of course, with Fairfax County in Northern Virginia. So he's an expert in the national Capital Region.

Mr. Souder.

MR. SOUDER: Thank you, Bill. Good morning, everyone. It's good to be here and I appreciate the opportunity.

I guess it's appropriate that I be the last panel member because it's really at the 911 centers in the nation that the rubber meets the road. And that's really what we're talking about today.

We talked a lot about, in the earlier panel, interoperability and I'm drawn back to the comments of Admiral Barnett at the outset when he said we're on the cusp of the next generation of

public safety communications. And he's absolutely right because really if you think about the current generation of public safety communications, it is largely driven by interoperability. That whole effort began with the Federal Communications Commission and it didn't begin post-Katrina and it didn't begin post-9-11. It began 27 years ago, a quarter mile from where we're sitting this morning, on a bridge that many of you may have came across this morning as you came to this building, when an airplane struck the 14th Street Bridge, went into the Potomac River, lost about 90 lives. And it really gave birth to the need for interoperability.

In the spring of that year, the FCC convened a session just like this -- and I mean, it's like déjà vu to me; just like this -- to say to the public safety community as they're saying right today, what do you guys need? And if you get it, how are you going to use it? And really that sums up what we're about here today. And the public safety community said back then 27 years

ago, we need more spectrum.

Surprise, surprise. And they gave us more spectrum. And that allowed us to build interoperability. And today as we come we're being asked again, what do you need? And how much spectrum do you need? And how speedy does that spectrum have to be for you to achieve what you need to achieve? And I think to a large degree we don't know the answer to some of those questions. We kind of have a vague idea about what we need, but how much spectrum we need to make that happen and how fast that spectrum has to be is still to be determined.

My mom and dad told me as a kid more is better than less and faster is better than slower. And I learned that lesson well. But it's hard for me to really define it in this arena because I just really don't know the answer to that.

For those of you who may have woke up this morning and live and traveled in our area, the first thing you do before you ever get a cup of coffee is you should turn on WTOP. And the

lead story throughout three broadcasts that I heard this morning didn't have anything to do with traffic but it had to do with the speed of the Internet. And what the announcer was saying, that in the United States we are four times slower in the speed of the Internet than any other developed nation in the world. So, Marc, you don't have to worry because we're too slow for the bad guys to do any harm.

(Laughter)

MR. SACHS: That's reassuring, Steve.

MR. SOUDER: But really, if you think about public safety communications, -until a relatively few years ago it was a three-legged stool. There was 911, in which we received the calls; there was computer-aided dispatch in which we processed the calls; and then there was radio that we dispatched the calls on. But we've added a fourth leg to that stool and it's called data. And data is really where the need for broadband lies. Admittedly, if we get b broadband -- and we will; we have it -- but if we get it in the amount

that we need and the speed that we need, it will impact the other three legs of the stool as well but it will clearly impact the data leg of the stool.

In my own county, we just deployed a brand new mobile data system. We do not have our own broadband network to operate that on. We are obligated to go to the private sector and compete and pay. Pay big time, you know. It's an extraordinarily expensive way to do business. But I would also at the same time challenge my colleagues in this room and around the country that when we say we need more, we need to be honest with ourselves in how much more that is. And when we need to say how fast, we need to be honest with ourselves then because we can't take something as finite as spectrum and just say give me all you got and I'll use it some way or another. You know, we have to be fair and honest to ourselves.

But having said all of that, my time is almost up. And again, I thank you for your time

and I welcome your questions.

MR. LANE: Thank you very much, Mr. Souder. And thanks to all of our panelists for your opening comments. At this time we'd like to go ahead and open the panel for questions and discussions as the topics may lead us. We welcome questions, obviously, from the audience here, as well as questions from those who are attending via the webinar. And also we'll look to our expert panelists from the government side of the house for their questions, as well.

I would ask that in the process of doing that, if you're in the audience here, please identify yourself with your affiliation prior to your question. And also, I would ask to remind folks to please silence your cell phones so we don't disrupt the answering that any of our panelists may have.

Let me begin by asking a question of our panelists and I'll begin with Mr. Souder because it follows on some of your experience, as well as the comments that you just provided. It also

hinges on some personal experience that I have from responding to Hurricane Katrina and the large-scale disaster that happened in New Orleans.

What are some of the specific planning factors in terms of broadband capabilities that need to be considered in view of a major disaster-type of situation? In other words, what are those broadband-specific things that we need to address for major disasters--the Minneapolis Bridge collapse, as one of our panelists could address earlier today, or a Katrina affair in New Orleans, or any of the other hurricanes that may affect the southeast region of the country? Major disaster-type situations. What kind of broadband-specific planning do we need to do in those circumstances?

MR. SOUDER: A very good question and very timely in many ways.

Any major disaster, regardless of whether it be natural or unnatural, is going to usually overwhelm the capacity of the local first responder community and they, in turn, are going

to have to reach out. They're going to reach out to FEMA and many, many other agencies that have been represented on these panels today and that are not even in this room. And they will respond to that emergency with a variety of tools of the trade. Equipment. You saw the mobile command post pictured earlier, and that's just one of many, many things that can be deployed today.

So, it's very important that there be adequate bandwidth to accommodate the multitude of devices and systems and communications technologies that are going to be brought to the scene of the emergency. Just to arrive with a truck, but a truck that can't have access, is to really bring an asset that has no value, if you will.

MR. LANE: So from the industry perspective, how would Verizon do that planning?

MR. SACHS: The continuity of communications is the key piece. So anytime there's a disaster, something that's unfolding, communications, a lot of times we just assume it's

there because it works so well. If you have a physical disaster, natural disaster, hurricanes and storms, a lot of times the communications -- because now we're talking wireless towers, things could be cut, fiber optics under bridges -- Verizon, AT&T, and many others that are your nation's communications carriers plan for and anticipate these things as best as we can. We try and provide that redundancy. The best thing that can be done is for those communities and localities to plan ahead, to think about what is critical, what does need to be replaced, what order, what sequence, so that as we do roll in communications, as we do bring in extra fiber optic and repair crews, we know exactly what the priority is. Where is the priority of service? What needs to be restored first? Otherwise, if we come on scene and it's chaos, we don't know. And we do the best we can. A best effort. But it helps if that planning is already done in advance.

MR. LANE: Moving across the panel then. From the Health and Human Services perspective,

how about planning for a major event?

MR. RAHEEM: Well, I would say two things. Obviously, planning for us is having access to the systems. But the other issue which we're finding more and more now is the prioritization on those systems. We're used in response -- and I'm putting on my pocket protector for a second -- is things like GETS cards, wireless priority service, TSP -- things that we brought to bear or private LMR that I know my frequency is my frequency and I, you know, go over to Charlie's guys and say give me 409 and they give it to me. Now, we show up at a Superdome event and Johnny and Johnny's mom and everyone else has a personal device that's now taking our bandwidth from the large available pool. So, if we show up to then use that bandwidth, how do we effectively use it where today I'm not sure those systems exist? And then how do we do it, obviously, securely?

If we're doing things like HIPAA data and Privacy Act data for medical transport, it's

pretty important to us to figure out ways to do that safely and securely. But also to ensure that it's integrity is maintained because the things of what we need to find out there -- the number of people, the fact that a space looks good, but only to find out the sanitation facilities are all not working -- that's critical stuff and that's all stuff that broadband can bring to bear. But how do we do that in this very stressed environment is the question we'd sort of ask industry more than us in a sense. So.

MR. LANE: Dr. Hooper?

DR. HOOPER: Yes. This is a very good question. I'll actually answer in a couple of ways.

Basically, natural disasters of flooding and earthquakes or other things, you could actually oftentimes plan ahead but today basically our disaster recovery is very much dependent on terms of communications. And basically, there's a kind of interdependency, for example, on the private networks versus public networks,

infrastructures that are pretty much interdependent. That is if you were going to plan ahead -- for example, one category of attack -- there are about 5,000 categories of attacks, you know, generally in terms of security and other attacks. But if you depend upon communications where you depend upon the Internet or let's say on the (inaudible) network or LAN, et cetera, and into the wireless area, the problem is how do you know that actually you've recovered the right type of data.

Say you have what we call a distributed denial of attack or sort of a denial of service, which means that you can't get access to communications systems and our data centers are not operating. You have a backup center but how do you check the integrity? Assuming you have what we call a "man-in-the-middle attack", okay, a lot of companies are doing this, recently Cisco, et cetera, and HP and others. But the problem really is that sometimes we're not really dealing with real traffic or real scenarios in real-time.

So we're not looking at real data in traffic.

What's happening in terms of the capability of somebody interrupting your service so that the challenges for us do what we call multiple backup so that you've got integrity of it and practice real scenarios. And then time it within five, 10 minutes and see whether you can come up to the real normal speed and see if you can test to see--this is actually the integrity we're talking about. You know, has it been intercepted? There are many attacks that have come across the world in different governments from Australia to the United States and Europe. Often we don't really know who is it that caused the problem.

So, I'll say that this is a major thing that we really need to do a lot of analysis and testing of our disaster recovery plans and the backup data centers, et cetera, and the communications systems which often are not really tested because you haven't really experienced real scenarios. So we're limited on experience and

often it's very costly, like Katrina, et cetera. So we need to do more scenario-type testing of our systems.

MR. LANE: Dr. Afflerbach.

DR. AFFLERBACH: I would say that all the different layers of networking are important but to start with the physical networking layer where you put in--in the case of fiber optics communication we have multiple physical paths. We have underground, as well as things that are on poles. We have -- and it's important as building things to high standards and so forth. Also, having knowledge of where all the locations of potential failure are. If you control your manholes, if you control the buildings or know of the buildings where you have access, where things can be reached, or where things can potentially go wrong, you're way ahead of the game. The Washington, D.C., network that we demonstrated here has a demonstrated uptime of five nines, and that's not just in the core--that's to the edge and that's the real record of uptime and

performance.

But in addition to the physical layer -- and in addition to the knowledge and control of the physical layer is in helping you in an emergency -- is also what you do when it's not an emergency. And when you have the kind of bandwidth that we're talk that these fiber optic networks provide it's literally as if every building in your network-- whether it's a government building, a police location, fire location, a school or whatever, is if it's all the same building potentially for purposes of bandwidth.

What does that get you? That gets you the ability to train much more effectively because you can train first responders in the station without having to take that station off duty and bring the first responders someplace else to train and to downgrade the protection of that particular neighborhood. You're able to do regional coordination across the region so that in this Washington, D.C., area where you have to take the

entire day off to come from Virginia to be involved in an exercise of the Council of Governments in Washington, D.C., and go back, where that can happen more frequently and less painfully because you've got the interactive communications network, the NCRnet, which interconnects these regional fiber optics is able to do.

You have fiber optic capability which allows you to have regular backups from facility to facility so that even though you've built a very expensive 911 center or data core network -- that that location is mirrored in some other location and potentially mirrored way off outside what we're calling the blast zone here in this area in Washington, D.C.

And you have the ability that if something has failed -- if you lose that building and it burns down -- you can recover to another location.

And finally, you have the ability that if you have connectivity to places like schools

and community centers, which you don't necessarily think of as your emergency locations, those are, in fact, your shelter locations. Those are, in fact, the locations where Mr. Raheem and his people are going to be coming in. And that's going to be the way that those folks ubiquitously are able to connect back on net and have that location not be a little isolated outpost but something that's just as much on the highway as a major location.

MR. LANE: Very well. Thank you very much. I turn now to either the audience here, our web folks, or to our government panelists. Please, Mr. Phythyon.

MR. PHYTHYON: Thanks. I know elsewhere in the FCC's work in developing a National Broadband Plan it's grappling with concepts of network neutrality. And there are probably as many definitions of that as there are people who debate it.

But is there a potential conflict between at least some concepts of network

neutrality and what we're talking about here? And to some degree I think this alludes to the question from the last audience or from the web, sort of how do you get out of the way of that ambulance? How do you make sure that emergency services are prioritized, in particular in a shared network environment. So I'm just wondering your thoughts about sort of how do we deal with the need for the security that you're talking about -- resiliency, priority services for the responders -- in particular in a mobile environment, but with the broader concepts of network neutrality?

MR. SACHS: I guess you're looking at me, right?

(Laughter)

MR. PHYTHYON: I'm looking at anyone.

MR. SACHS: I'll go ahead and take the first stab and the rest of you can join in after me.

A lot of it really does depend on, as you say, how do you define network neutrality? If

it's only the Internet -- of which the networks are much bigger than the Internet -- if it's only limited to the Internet, then many of the things you're describing -- priority service and whatnot -- can be done outside of the context of the Internet.

If it's the entire network -- everything from fiber optic to satellite, to microwave and all -- it makes it a very good target for adversaries. As soon as we try and make things flat and neutral and unmanaged and we can't do priorities, we're sitting ducks. So what I would hope we would do in this conversation as we move down -- if we consider the Internet, there's probably a lot we can do there -- where we can have that good conversation about what does it mean to be neutral. When we talk about priority services though, particularly managed services, private networks, wireless, things that are not the Internet, that conversation then does need to lean towards managed services, priority, working with the first responders, figuring out what their

needs are.

So there's room for both and this is the type of conversation -- we need to have a balanced conversation with the needs of both sides being represented. And I think we can achieve what both sides want.

DR. AFFLERBACH: I think I'd like to add to that. Our communities in NATOA have been involved with the BTOP application process and have entered the first round and submitted -- and as you're aware, the BTOP has a requirement for neutrality in the infrastructure that's being built. The local governments want to build these networks and have considered how neutrality would work in each situation. And it really isn't a one size fits all. But in some cases the most robust approach was to basically put in enough fiber optic strands so that when Verizon or when other carriers want to have access to the network, that they're able to access through manholes and meet me points and so forth where they're able to have access but it's on separate fiber optic strands

from the critical networks that would be put into place for public safety or what the other providers would have.

In other situations where for many reasons the extra fiber strands were not in the offering, the engineering called for using electronic separation using MPLS-based technologies and in using provisioning in a way where once again you had public network space, you had untrusted, and you had trusted networks essentially that were kept electronically separate from the design. So there's no one size fits all but approaching it in a careful approach with people who are experts in cyber security and so forth, we can try our best to build separate spaces for neutrality and for public safety.

DR. HOOPER: Yes, I read a very important point here. There are a lot of issues here in my consulting in the last 20 years. It has been interesting to see that companies actually work together when it comes to emergency services. There's obviously competition. For

example, IBM has different data centers. AT&T work together in Belgium. There are about 20 data centers. And I found that actually when traffic travels, oftentimes you get to what we call bottleneck areas where we can't really travel without cooperation with other networks. So you get what we call kind of a trusted and untrusted area.

Companies are not -- for example, Cisco and other companies and major corporations -- (inaudible) willing to give a lot of information without cost effectiveness and operating cost effectiveness. One of the challenges is to ask them is it cost effective to us? Can the government actually pay for those additional fiber optic networks? And are we going to trust them? Are we going to secure them? Who is going to pay for that? In terms of the business side, intensive security and real intelligence, I think it comes to a point of whether or not you trust the administrative people on both sides.

I'll give you a scenario. For example,

in Belgium or other countries in Europe -- other data centers around, say, (inaudible), et cetera -- you have different networks coming to the same data center. Well, who owns that network?

If you want to get one of those networks or let's say a track for emergency services, can we take that and trust that administrative personnel to monitor that effectively to really secure it for us? And after it's finished, what are the issues of securing privacy around that? You know, what kind of data has traveled that network? And can we guarantee that it can actually look at real traffic for us and secure that infrastructure for the future?

So, we've got issues of, first of all, neutrality as far as in terms for the public good. Okay, we have competition. We have actually disaster recovery, et cetera.

But can you really trust companies and private networks to give you their data and share it in real-time? And are they prepared to handle that because already they have their own burdens

of traffic handling and they cannot (inaudible) real- time?

So I think what it is is that we have to have a strategic approach where there's a hybrid approach. You have both the companies, their own private networks. You've got dedicated lines that can be open exclusively for traffic. We monitor that very securely because that's where it opens it up for hackers and other student hackers to find out about that. And then we also do a shared approach whereby you kind of compensate them when you use their networks for emergency services. And on those traffic -- or let's say three parallels, you have to really train people. Make sure you know their identity, the integrity. Make sure you know the private side is not compromised by hackers -- let's say (inaudible) interest personnel. By the way, about 75 percent of real breaches come from internal -- the person who leaves and goes somewhere else has a grudge or et cetera. So you have to really look at integrity issues, whether or not they're interested in

common good as a whole, and study that kind of data and see how you can really adapt it over years. It's kind of something that adapts as you go along overall.

MR. LANE: Any other comments on the question? The questions are coming in fast and furious.

Keep them coming. Thank you. Let me move to another one from a member of our audience here and I'll go ahead and read it as well as paraphrase a related question.

The cyber security issues are real and a serious threat. They would imply that public safety agencies should build their own independent broadband, both wired and wireless networks, rather than use the public networks or commercial networks. This leads to the question that the public safety community and the military share and that is one of assured communications, which is critical, obviously, for our first responder community. But it leads to the question of separate networks or the related question from a

cyber security perspective, can our public safety networks be secured or must we rely on independent networks?

DR. AFFLERBACH: I would say that nothing can be perfect. I mean, as quickly as we can come up with security mechanisms to protect, the bad guys can essentially come up with something that they would get us. But I think that of necessity, just because of cost effectiveness, there has to be some kind of a balance between what is done by the government and what is done by the private sector. In any case, the government, even if it is a full government implementation, is going to be bringing in contractors to do the work. So that's still a public-private partnership of a sort.

So I guess what has to be developed, I would say, are standards of what constitutes acceptable risk. We have to have best practices as far as the physical security of the electronic security. We have to have the best minds and efforts as far as proactively being in front of

the threats.

But, again, I think it's case by case, network by network -- what is acceptable and what practices we put in place. And that's what determines in each part of the network what balance to strike between the public safety only and the network provided by the private sector.

DR. HOOPER: I think this is a very, very good question, perhaps at the center of this whole cyber security infrastructure effort by the White House. Incidentally, it's interesting to see Melissa and others do the research and also have the speech by Obama on the topic.

I'll say that historically what's happened so far is that the hackers will get in from around the world, whether China, Russia, et cetera. They're not really coming necessarily through the military networks, et cetera; they come basically from the private networks that the military and the other intelligence agencies cannot really help the private regulations and privacy issues prevent them from monitoring those

networks. So those hackers are very astute about this. Much of the traffic I've been capturing across different global networks (inaudible) to the United States in and out really comes through what we call the -- kind of what we call benign in terms of the private industry sector but interfaces with the contractors and agencies that work for the intelligence community, et cetera.

So what is happening is that basically you face a couple of challenges. One, should you continue the public- private partnership and bring contractors to do the work? Because it's cost effective and also it's too expensive for the government to manage building their own design and become an industry of itself. However, there are ways to address this. One is basically there might have to be a regulation passed. I'm really challenging this because the hackers can come through private networks into the intelligence networks.

Let's look at an interface between those two. How do we really allow contractors of

private networks to come in and actually do work for the government and yet be kind of a back door for hackers? Or should we legislate or bring kind of an experimental approach where we have a dedicated network that's completely separate from private networks. And actually, monitor that and look at its cost effectiveness over time because the reality is that, you know, the 21st century for the United States' security is not just local security but actually intelligence gathering of the capability of the United States of counterintelligence--what enemies know about your capability and your limitations.

So, the answer is both. You really have to bring in sort of a dedicated analysis and research into what is the capability of the dedicated network when you actually build a separate network? And how can you protect that from private, let's say, loopholes or backdoors? No matter what you do there will be a backdoor. There's no doubt about that. You can't be completely exclusive. There's some kind of

interface. However, you can actually secure that interface by monitoring the traffic in real-time. Don't talk about unintelligent (inaudible), you can't look at it with your naked eye. You've got to really look at it in terms of intelligent (inaudible) attributes, what we call intelligent events.

And that's what we like today. We don't really have a very good monitoring system. The looks at what's happening in real-time. So most of the things that happen, you don't actually see them. They're not logged at all. There's no log sessions at all so you can't even see them. So we have to really be astute to build intelligent and secure systems that can actually adapt and have algorithms and methods. Many products are actually doing this but unfortunately didn't have intelligent algorithms. And we need to log that and then reevaluate the performance and actually bring about a system that can be resilient for the next 50 years.

MR. RAHEEM: I would say to a great

extent, at least from what we see, that genie is already out of the bottle. I mean, we think the network is private. We build the repeater site and I call Verizon, for example, and say give me a circuit switch thing. But more and more, the networks -- we're not watching what the black magic is that's happening behind the scenes. That's no longer an actual circuit. That circuit terminates in some sort of gizmo that gives us packets out the back end and it goes in a larger network.

And we feel that it's private because we plug into a plug on a wall, but that doesn't apply anymore. And I think for your economies of scale and LTE and all these technology we hear about, it doesn't apply anymore. So how do we ensure our networks are safe and interoperable? Because it's very easy to go into the sort of mode of I want my Op Center to only talk to your Op Center and go across a wire. But it doesn't work anymore and I think it's one of these challenges that how we face that is really the challenge, not keeping it

all quiet and private. It doesn't apply.

MR. SACHS: The question tees up about six answers, so let me just be brief with them because I can spend an hour talking about each one of them.

First off, the networks are not just the physical world; they're not just the virtual world; it's not just applications; it's not just protocols. It's a little bit of everything, including people. The private sector and the public sector depend on other infrastructures together, like highway systems. They are virtually no highways that are only to be used by ambulances and police cars and the people can't use it otherwise. We share that infrastructure.

The electric grid is the same way. There's very little of the power grid that's uniquely just for first responders. It's a shared infrastructure.

Coms works the same way. The physical side of it -- the fibers, microwaves, wireless and others -- are a shared infrastructure. Could we

build a private one completely that's just for government use? Of course. But at what cost? And who maintains it? And who engineers it? And who does those long term things? This is where we get a lot of cost savings by using the private-owned or the commercial networks and then we provision from there. So the private circuit you're talking about--it used to be in the good old days you could order up a T1. You could have an actual--no kidding--you could walk that piece of copper all the way through and it really did connect to the other side.

Today it's really the cloud. You order up your T1 and it's a piece of copper up to a demark point, hits a switch, and then it just becomes cloud after that. It still works the same way and the customer on the end doesn't know much different. But our adversaries don't really care whether we separate this out into private networks. They don't care if we bring it together into a cloud. Adversaries work for us. A point was made about the insiders. Adversaries are on

the outside. There is a problem the DOD faced a number of years ago with the assumption that their private networks -- since we mentioned DOD a moment ago -- were much more secure and much more resilient because they weren't connected to the open broad internet. They found out the hard way that's not the case. That now where an evil spreads on those private networks actually better than it spreads on the public Internet because there's far less security. The mindset is not there. We don't have all the circuit breakers in place.

So don't fall in the trap. This mindset that says if we can just build private separate networks then all will be safe. What you might wind up building is a private separate network that truly becomes a soft underbelly. That becomes the Achilles heel. That's what fails. And then there's no fail over to the commercial side, no quick way we can move over to a network that is more adaptive, is more resilient, better managed.

So we've got to work together. This is a conversation we all need to have in terms of costs and in terms of resiliency. But the idea of building physically separate networks, I think we learned that lesson years ago.

That's probably not cost effective and certainly would introduce even more security problems than the ones it would solve.

MR. SOUDER: Last week I was at a conference of APCO in Las Vegas, and again this year as it had been for the previous two years, both formally and informally, one of the hottest buttons talked about was this very issue. Not so much on the cyber security dimension of it but the more core issue of in today's world do you own your own and maintain your own or basically do you ride on someone else's network.

There is no easy answer to it but certain I think the points that Andrew made at the outset are very, very appropriate. If you went the traditional route of building your own, could you really afford to maintain it? Are you going

to be able to maintain the personnel base to maintain it in today's world? Are you going to have access to the latest technology the way the private carriers would have? These are questions that really have to be honestly weighed.

Certainly, our telephone system is a prime example. Very few communities own their own telephone system. Look at the water supply system, you know. And I could go on and on and on.

But clearly I think what public safety has to develop a high level of comfort with is that if they do go the public route -- if they do subscribe, if you will -- that they are absolutely assured that they have the security: Physical security, technological security, latest technology that they would hope to have if they could afford to do it themselves. So the challenge really is to you guys, if you will, and your respective companies to provide to us guys, if you will, scattered around here, what we really need to give us the high level of comfort to look

at things differently in the future than we have in the past.

DR. HOOPER: I think I would like to add one quick point about this. This is a very excellent point. It's not so much the networks but actually the technology. And I think this is where there's often a challenge between commercial research and academic research. Sometimes academic is way ahead of commercial, and commercial (inaudible) business, ([inaudible), and the government provides the financial means for the commercial to continue.

But I think a very good point is that the government is relying on intelligence -- let's say intellectual and very much improvising -- improved performance from the technology that's available currently. Unfortunately, hackers are our arch-enemies (inaudible) vulnerabilities in the technologies themselves. So you have a dependency from the military on the commercial or let's say the industry. And the industry is actually looking at a commercial way of benefit

from the research. Is it valuable to them? Can they benefit? Can the companies actually pay for it?

So you have to really have a kind of partnership between the research that is funded by the government but also by the industry so that both are actually benefiting from this. Because without those two in parallel, basically industry is very much behind what the challenges of today's, you know, security issues are concerned. So, for example, the United States is actually behind Russia and China in terms of astute manipulation of technology. You can have a standard policy technology but you need a kind of way of looking at how to--the vulnerabilities of those technologies and the capabilities because that's what a government depends upon. And if you do that you can actually look at how to improve products -- applications, security, IPS, intelligence -- let's say emerging systems. Unfortunately, what we have today is not very adaptable to emerging challenges we face with 21st

century data traffic and high-speed data and a high obligation of data in real-time.

MR. LANE: Very interesting comments. Thank you very much.

Prior to coming back to our colleagues from the government side of the house, there is one question from the audience that I'd like to entertain at this time. And it really takes us in a little bit different direction with regard to broadband applications. Please.

MS. CLARY: Good afternoon. I'm with the Minority, Media, and Telecom Council. And I'd like to tack on to the conversation earlier about Hurricane Katrina and ask that the panel please advise the Commission that one of our emergency communications needs cannot be met by broadband alone.

During Hurricane Katrina, the electric grid and cellular towers were down, and for the many people who were on roofs of their home because of the rising water, terrestrial radio was the most useful technology to them because some of

the stations were still in service and most people had access to battery-powered receivers. However, during Katrina the only Spanish language station serving over 100,000 people who had no English fluency was knocked off the air and the English language stations did not provide emergency alerts in Spanish. As a result, MMTC filed a multilingual radio proposal with the Commission, and the next year the Commission's Katrina Advisory Committee unanimously recommended prompt action on our proposal. However, now four hurricane seasons later the Commission has still failed to act.

Could the panel please advise the Commission that it should not rely solely on broadband to solve the problem of multilingual emergency communications, and therefore, the Commission ought to focus on other technologies, particularly radio, to ensure that all persons, including those not fluent in English, have access to life-saving information before, during, and after an emergency.

MR. LANE: I'd like to, prior to presenting the question to the panel, expand that slightly to go beyond just the multilingual requirements of citizens but also to the disabled community. So how can broadband support those requirements as they may come up in an emergency or a disaster situation?

DR. AFFLERBACH: I think actually circling back to the question, I would say that the broadband has a role but we have to remember that we only have what we have when we're running out of a Katrina-type situation and we're in vehicles and we may have power for only so long and we may only have the radio and we may have language issues and disabilities and so forth. So what's happening with a number of communities -- Arlington County I'll put up as an example -- is going back to some of the old ways of communication. An AM radio station where there are signs on all the major corridors that in an emergency information will be there in English and in Spanish for how to get out.

The other thing that Arlington has done recently is put up air raid sirens and speakers and so forth to get the word out about evacuation; to get the word out about where there's water or ice or things like that available; and then, of course, other techniques that -- broadband enables this to some people. You can have alerts going out -- text messages, e-mails, and so forth to some -- but I think that what I see happening is some of the communities that are doing, I guess, local homeland security -- groups where people are looking out for their neighbors -- those individuals maybe are the higher tech and get that information and look out for others who may not be adept in that area or may need the help and then go and knock on doors and so forth once they get their roam secure text message or whatever broadband is used to help get to them and then they pass the word on using low tech.

So, again, I agree. Broadband doesn't bring the full thing to the table but can do an ancillary role.

DR. HOOPER: Yes. I think these are very good questions. I will say that actually picking up from disabled, but also different languages as this country is very much multinational. Different languages, translation, et cetera.

I think it could actually do a lot of things here in terms of not just the high-speed broadband but looking at it in terms of what is available right now and maybe dedicate actual certain frequencies for specific messages and test those. Different languages. Look at different areas of the United States and find out where the population doesn't have a high representation of local dialects. There could be different languages in different areas such as, for example, in Chicago there are different types of people. If you go to Los Angeles or California you see different than Massachusetts.

However, sometimes people learn second languages. You know, adopt. So you can kind of look at what kind of languages--you can actually

get a certain feel for second frequencies in radio transmissions. Dedicate that to, let's say, messages in the case of an impending potential disaster.

Another one is look at disabled, for example. People cannot get out of the room, for example. What would you do besides broadband? Well, again, radio and perhaps training people, having visitations from different social workers, for example, visit homes and train them how to use other frequencies, radio channels. Or perhaps dedicate that to specific usage in different communities. And in this case you actually provide for them what available frequencies already exist in terms of radio transmission, dedicated messages, et cetera, and train them how to use that. That would make it possible for them to adapt and maybe do some drills and visit the homes and see how they're actually doing. That costs money, by the way so you have to kind of work with local and state and federal agencies and see whether or not you can actually budget

something and make it possible for them to really, you know, practice in real-time.

DR. AFFLERBACH: One comment I'd like to throw just to add to what I had said before. The way that the FCC can help in this instance is that Arlington County and Howard County, as well, were able to obtain waivers to operate on the Travelers Advisory Radio spectrum that is usually reserved for much lower power. And they were able to go to higher power to cover their service area. So that's an instance of how FCC can help in this instance.

MR. LANE: How about from Health and Human Services?

MR. RAHEEM: What I would say what we all found from disaster response is don't let perfect be the enemy of the good. I think broadband is something we all want because it brings a lot of very rich things to the table, but the more--and I'm sure hopefully Steve would resonate with this-- but the more tools we have on the belt the merrier. I mean, yes, we need

broadband but we need LMR. Maybe leaflets are good. Maybe the cop car with the PA system on driving down the street will work. I mean, the more things we can bring to bear on any of these scenarios, the better the outcomes are. And I think it's no one technology. Obviously, this is broadband. Its discussion is relevant to everything but the more we have to do with stuff the better we can prepare.

MR. SACHS: Just a brief policy answer, something to think about is broadband, in time of an emergency, it might actually be more effective for people who are not in the emergency area. In other words, during Katrina you've got millions of people who want to know what's going on. They're dialing their friends. They're flooding the phone lines. And so we have a collapse of inbound calls. Broadband can allow us to put the message out so people that are outside the affected area get real-time, up-to-date. We know what's going on so they're not calling their loved ones to find out what's happening.

In an affected area, if broadband is beginning to fail, if we're having cuts and things and towers have collapsed, if broadcast AM/FM is working, as all of you know, over on the FM side we've got digital subcarriers. If you've got a fairly late model car your radio inside tells you what you're listening to. I mean, there's a digital signal coming through there. There's nothing in the world that says that can't be multilingual. There's nothing that says we can't find -- you all see these little first responder radios that you can crank up and you can use during a storm. Put a little LCD display on it so it can also display text in multiple languages that could be broadcast over FM.

So that's a very inexpensive low bandwidth kind of solution for people in the affected areas. But maximize broadband outside the affected area to get the word out, to let other people know what's going on so they're not flooding the networks or even trying to physically go there when they're not needed.

MR. SOUDER: Building On Murad's comment and the original question, he used the word tool belt. I was going to use the word toolbox but we're both talking the same thing. Public safety communications is a set of tools, ever expanding, if you will. Rarely do we drop anything. We always add to it and that's the way it should be.

But at the same time, voice recognition technology today is on the brink of a huge breakthrough. And I've heard that Google is about to do something that is just going to be revolutionary. I'm not quite sure what that is but it's going to provide an opportunity in our increasingly diverse country for ourselves to use the existing technology but to apply it in a set of text and words and languages never before realized. So it's very exciting and it's a very good point that was made from the floor.

Thank you.

MR. SACHS: Let me add to Steve's comments. There are translators now in Iraq that the military is using -- have you got one?

MR. SOUDER: Yeah.

MR. SACHS: So those are fascinating devices. You just hold it up, you speak to it in a foreign language, it translates back into English and vice versa. Those are wonderful pieces of equipment. What we need to do now is take that military technology, bring it back home, and deploy it at the local level so you have it ready to go. Obviously, it's not going to speak Iraqi necessarily. It would be probably Spanish to English and French and German, but those technologies exist. And then take the next leap, make them wireless so that you can then communicate at a broader level besides just one-on-one.

MR. SOUDER: And not to digress from broadband, but I would estimate that in our lifetime 911 calls today that are received every day across the country from as many as 100 different languages and to which we always reach out for an interpretation service to provide that third party interface to give us the

interpretation of what we're hearing, there will be a day in our lifetime when voice recognition technology will take that spoken voice, translate it into English, if you will, and then take the English speaking call taker's voice and translate it back to the language that was spoken. It will happen.

MR. SACHS: Oh, yeah.

DR. HOOPER: Yes. Actually, there is some technologies, technologies that actually developed in the last 10 years where you actually can take approximately about 200 languages and you have adapted language software that actually writes and interprets back to you. This actually began about 20 years ago. I worked on a project like this. But there are more advanced features that you can actually now in a very, very short time take a message and just translate it using software and voice and pattern recognition and very quickly change that into an interpretable language.

So much of the messages now are actually

machines talking to you.

You can also get messages over wireless. Today if you have a wireless network you can just connect. You don't have to actually use a telephone so it's actually much cheaper that way. So there are a lot of ways to use that and change that into a kind of a multi-pattern changes in real- time.

MR. LANE: Let me exercise moderator privilege here and turn to my colleagues in the Commission and government if they have any questions.

Charlie, please.

MR. HOFFMAN: Thank you. Deep in the bowels of FEMA, down in the apocalyptic planning section in the basement, we have to think worst case scenarios on our planning. One issue that we're struggling with now is this little fault that runs from Missouri up to Indiana called the New Madrid. This -- if this should happen -- we can't get the geologists to tell us whether it's a 200-year event or a 500- year event. We're hoping

it's a 500-year event, but if it's a 200-year event, it happened in 1811.

So this, if it happens, could essentially, communications-wise, separate the East and the western portion of the United States -- not to mention disrupt our lines of transportation, shipping, whatever -- because the last one that happened caused the Mississippi River to flow north for three days. Okay?

My question is should the National Broadband Plan address something this drastic? Is it something that as far as built in redundancy and reliability on our broadband networks -- because should a disaster of this magnitude happen -- I mean, we're having a hard time getting our hands around planning for a disaster this huge. It would totally and very easily could consume our capabilities within FEMA to provide reliable communications across the chasm that could be created by this disaster.

So this is something I'd like to present to the Board. Is this something -- the panel, is

this something that we need to be looking at very seriously on the commercial side as far as how far does our redundancy go? How far does our reliability need to go? Or is this something that it's probably not going to happen for another 300 years?

DR. AFFLERBACH: I guess I'd say the good news is that this might be one of the easier problems to solve of the many that would be out there after such an event. One of advantages of the fiber optic communication -- and there are many other technologies that are available -- is that any one cable is going to be able to carry the capacity of everything that you had there before. So, if we have an architecture that's significantly mesh-like with respect to roots, with respect to different carriers, with respect to maybe failover to going the other way around the world or whatever have you -- that's, I think, something that you'd want to put on your list of capabilities for any survivable network that had to absolutely be up, as well as public network

being able to somehow make do and make it continue in that situation.

And the other things that could happen -- massive cyber attacks, loss of key facilities that would require the same sort of capability (inaudible) -- but like I said, the good news, you know, compared to the multitude of other horrific things that will have to be taken care of is that there are a number of technical solutions that could make us whole in that situation.

DR. HOOPER: Yes. I'd like to say actually it's a very good question and I think we can expand that question further. That's the major thing. Oftentimes, we need a major disaster for funding to come in or new policy to be changed, and that's actually what has happened in the past.

But this is quite a challenge. I think one thing to consider is historically the United States infrastructure was developed over different rivers, different parts. It was not really designed with a long-term future in mind. It was

kind of a short-term need and then it was added on incrementally. You had a huge infrastructure that had inter- connective (inaudible). So if you go to historically the eastern part of the United States you see a lot of that pattern (inaudible). For example, in New England, et cetera.

If you go to the West Coast and the Midwest, it's expansion is much more planning ahead.

So I think all we need to do is have a strategic planning -- kind of a study, if you like -- of what are the infrastructures that exist today. For example, the one they have in Minnesota, they didn't plan and look at how did these bridges get built. You know, in New England there are many bridges like this. And what would you do if a disaster took place? We need kind of a proposal that Congress will fund this and say, look, let's study the history of United States' infrastructures. Why were they built? What were the purposes of these functions? What are the capabilities of the time? What are the changes

over those periods--in the last five or 10 years? What are the geographical layouts and the physical locations? And what are the seismographic analysis? All kinds of satellite imagines are telling us where the weaknesses are, what are the points. And what is the age of these infrastructures? What are their limits? Because, really, frankly, most of these infrastructures actually have not been maintained even every two or three years. They just wait until an inspector goes by and there's a lot of poor inspection, as a matter of fact and data is not gathered in real-time in terms of thresholds and limitations.

So we need to do really an historical and incremental study and look at different kinds of risks associated with those vulnerabilities and, let's say, weaknesses and different points there. And actually come up with a budget and say let's begin to plan ahead and actually fix -- for example, disaster recovery and resilience, you know, different kinds of places where you can actually put different backups, et cetera, and

recover back in real-time.

Those are actually not in place in many places because there's not--there's no funding and also there's a lot of, let's say, overload. So you can't really use that for disaster recovery. Many of them are not working -- actually, operating effectively.

So when we get into Smart grade and other kinds of add-ons, we get into a reality that actually we are way behind time. So woe have to update our critical infrastructures, prepare for just the kind of functionality that it was prepared for, then look at, let's say, the cyber security issues which is way beyond that. However, the interface between the old and the new technologies are coming up pretty fast. So before we add on to those, we need to go back and actually improve the existing ones. These are new locations. We put infrastructures for really backups and recovery and then we can say, okay, now if this disaster one takes place, this is backup one and it's going to take care of that, et

cetera. An increment. All that kind of plan and then say, okay, we're ready to test it. You know, not to plan an emergency; we'll actually test some scenario-type events and then come up with the results analysis and go back and improve on it. Because you can never predict the magnitude of the impact but you can kind of prepare ahead of time for different kinds of scenarios.

MR. RAHEEM: I would say that, at least from HHS's point of view, the planning for the truly catastrophic is often useful. I mean, four years ago we were doing pandemic and no one was talking about that and we had to drag people kicking and screaming to the table. Things like New Madrid, which we've certainly been talking with you guys about, sometimes helps us not fight the scenario. If we're talking about a small event, if we're talking about a localized event, it's very easy that folks get very lost in some of the absolute nuances of, well, yes, but this street is working; this is not. Sometimes, like in New Madrid, if we're all speaking about it, at

least from our point of view, it allows ideas to be discussed which may not otherwise be discussed. And again, you know, when pan flu was avian flu people said, yeah, that's nice but it's happening over there. Now that's sort of changing so I would say we should keep focusing on it.

MR. SACHS: I concur with Andrew's comments. And in fact, I would probably feel at home in your evil basement helping you think of evil things.

It is really good -- we have built a very robust mesh-style network, so if you have a shift north-south ala Madridor you have a shift east-west, we've got connectivity that can route around that. And the point of having gone to fiber and glass is the capacity is just enormous.

I think your biggest concern there will be trying to fight those who feel that all the fiber optic cables must cross underneath the very same bridge. The only bridge that fell down across the Mississippi River shouldn't have even fell down. That used to be the case, that there

were limited crossings. The same thing through the Rocky Mountains. We had definite choke points. That's long been engineered out.

So now if we do have even something as severe as a multiple state earthquake -- and even in California, we haven't seen ones that go across, you know, multiple state lines -- but should that happen, the Coms infrastructure is built where we can route around that pretty quickly. You will certainly have local outages. That's to be dealt with on a different scale. But separating East and West United States, I don't think that's an issue the way we are currently engineered.

And we do get to test this routinely in the Pacific when we have undersea slides. There are cable cuts that are routinely happening. There are local outages but we don't separate the planet into two halves. And so fortunately, we can learn from those episodes and that gets us more resilient towards the type of things you're planning for.

And God bless you for planning for it. That's one heck of a scenario.

MR. SOUDER: And I'll wrap it up by saying in the 9-11 world there's something called vicarious liability. And what that translates to is if you know something is going to happen you better prepare for it. Well, you've introduced us to something that could happen that I didn't know about until this morning. But I like Andrew's solution to it. So consider it a done deal.

MR. LANE: We're rapidly approaching our closure time, so I'd like to pose -- and I have a number of questions still on my table and perhaps in others' minds as well -- so in the next few minutes if we could just do a short blast of single questions and maybe to a single responder we can approach a couple of questions.

First, any from my government colleagues?

MR. PEHA: We've heard a number of scary things in terms of cyber security threats. I'd like to ask a little about responses. Particular

-- Dr. Hooper, for example, has many calls for more research funding as a way to deal with this. I mean, we do have research funding. Are you suggesting different levels of funding? Different topics of funding? Different forms?

And quickly to Mr. Sachs, who talked about industry responsibility is to analyze and help mitigate security breaches, I'm sure, you know, Verizon is doing its best within its network, as are the others, but this is a network of networks. Are there other things we can be doing across networks that maybe we ought to be worrying about?

MR. SACHS: Yeah. I'll just briefly answer you since I know we are running out of time.

We've got a pretty robust response team that works not just inside our networks with our customers but even with other customers. Law enforcement will come and ask us because they're fairly well known. What they've developed is a very good body of knowledge about what causes

attacks, why people get broken into. They're building a framework of analysis so that when others do investigations they can follow that same type of framework.

This is a new mindset now that says that security is something we deal with. People will break in. One hundred percent is not there. So can we at least set up some type of framework where we continue to learn, we continue to improve? And it doesn't matter where the event happens. We're all doing it the same way in terms of providing rich information back for future improvements. And I think we're making a lot of headway there. And this is good. This is something not just Verizon but others are doing as well, and a lot of crosstalk in terms of lessons learned because we recognize the seriousness of this and the criticality of our nation's future on making these digital infrastructures work and work securely.

MR. LANE: Dr. Hooper?

DR. HOOPER: Yes. Actually, what we

need to do actually is not just pour more money into research but actually do the right kind of research. Twenty-first century intelligence is way beyond the 20th century because actually we're adding to problems we have never solved in the 20th century. And there are new technologies coming up in the 21st century we haven't actually studied enough about.

So what we need to do is actually study about what the high-speed environment capability is going to provide for us in terms of both functionality and also in terms of the challenges of, let's say, intelligence and counterintelligence. What I mean by that is basically what do our adversaries actually know about the products that we're developing right now and what is the capability in the future? Because frankly speaking, the 21st century, if you look at what has happened right now, there's not much study at all. Much of the products we have -- I'm talking about networks and other kinds of systems -- the log-in systems that we have today cannot

look at traffic, high-speed traffic in real-time.

Most of the IPS, IDS, and intrusion prevention response systems, there's so much metadata transfer across data centers all over the world and to the United States in an hour. Nobody's looking at them. Okay? They're looking at it and looking at the wrong data, or in fact, the student hackers are really happy about a lot of data. Why? Because they can hide there and there's no trace. There's no traceability. There's no log. A lot of algorithms and data projects at MIT and other schools, they're not looking at real-time traffic that is happening (inaudible). I've been logging this, in fact, for 24 hours in the last several weeks. And I've seen traffic that is incredible. The people -- I say, look, here's one right here. It's gone in five seconds. You know, so we need to study what is really happening in real-time that has actually been silent in the last few years.

So, the right kind of research is what we need to fund. And we need to really look

forward to the 21st century intelligence gathering and what is called adaptable algorithms in real-time so you can actually capture student hackers and respond to them in real-time. And that's what we need to fund so we can be ready for, you know, the 21st century 50 years from now, God willing, or 100 years from now. You know, not try to be behind all the time as we've been in the last 20th century.

MR. LANE: Are there any very quick questions from the audience?

MR. GOJANOVICH: My name is Bob Gojanovich. I'm with RCC Consultants.

Just to bring the focus back to the consumer public side of broadband for a moment and leave the major earthquakes and disasters aside for a second, we heard this morning about -- and Steve Souder can back this up, too -- on average, about half the calls showing up in 9-11 centers today are wireless. Some of those calls show up with a pretty good location; some of them show up with a pretty bad location; some of them show up

with no location. It's not a perfect science yet. Add to that text messaging that is so popular among young people; that people want to use for dialing 9-11; it's not real-time; there's no location with it.

Twitter, WiFi networks, WiMAX. There are no requirements from the FCC for location capabilities on WiFi and WiMAX networks. And as these things proliferate and people have more and more access to broadband, there's more and more devices and more new methods that pop up every day of how, you know, that give you the capability to report an emergency, get into the public safety information system. And more needs to be done. What more can the FCC do to require location? And how can we get better location information to the growing percentage of calls going into 9-11 centers that come in without it?

MR. LANE: Very quickly, Steve, would you address that one?

MR. SOUDER: It is a problem. And focusing on texting, if you will, in today's

generation -- and probably that includes many of you -- I mean, it is the preferred way of communicating. And the expectation is by those texters that they're going to be able to communicate with 9-11. Well, I mean, aside from the location issue which is a huge issue, you know, it's the ability to kind of interrogate and hear the background sound and all of that stuff that makes for an effective way of processing a 9-11 call. So it is a very, very large issue.

In our urban area, I don't think we have as much of a location issue, regardless of the device used, that might prevail elsewhere in the nation, but we have our pockets. And many times it does pose a real challenge for us because we have a lot of transients. And if they're in one of those pockets and they don't know where they are, we don't know where they are. It's kind of a throwback to where we began with wireless 27 years ago. So very good point, Bob.

MR. LANE: Unfortunately, we've come up to the time that we had planned to stop this

particular panel. First and foremost, I'd like to apologize for the number of questions from our webinar participants that unfortunately we didn't get to. I apologize to those of you here that we didn't get to any of your questions. I'm sure our panelists will be happy to entertain your questions afterwards.

But at this time I'd like to extend my personal-- and please join me in thanking our panelists for their participation today.

At this point in our program I'll return the master of ceremonies charge back to Jennifer Manner.

MS. MANNER: Thank you so much. And I just wanted to say in closing, thank you very much to all of our panelists and our government participants today. And, of course, to the audience, both here in D.C. and on the web. The presentations and the transcript from today's session will be posted on the website if you're interested.

And so with that I'm going to close this

session.

(Whereupon, the PROCEEDINGS were adjourned.)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

/s/Carleton J. Anderson, III

Notary Public in and for the
Commonwealth of Virginia
Commission No. 351998
Expires: November 30, 2012