UNITED STATES
FEDERAL COMMUNICATIONS COMMISSION

IN THE MATTER OF:)
)
TECHNICAL ADVISORY BOARD FOR)
FIRST RESPONDER)
INTEROPERABILITY, PUBLIC)
WORKSHOP)

Pages: 1 through 143

Place: Washington, D.C.

Date: April 23, 2012

HERITAGE REPORTING CORPORATION
Official Reporters
1220 L Street, N.W., Suite 600
Washington, D.C. 20005-4018
(202) 628-4888
contracts@hrccourtreporters.com

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

IN THE MATTER OF:)
)
TECHNICAL ADVISORY BOARD FOR)
FIRST RESPONDER)
INTEROPERABILITY, PUBLIC)
WORKSHOP)

Room TW C305
FCC Building
445 Twelfth Street, S.W.
Washington, D.C.

Monday,
April 23, 2012

The parties met, pursuant to the notice of the Commission, at 9:01 a.m.

APPEARANCES:

JAMES ARDEN BARNETT, JR., Chief, Public Safety and Homeland Security Bureau

CHRIS ESSID, Director, Office of Emergency Communications, U.S. Department of Homeland Security

BOARD MEMBERS:

STEVE PROCTOR, Executive Director, Utah Communications Agency Network.

COLONEL KENNETH C. HUGHES, JR., (RET), Regional Communications Coordinator, New Orleans Urban Security Initiative

BRIAN SHEPHERD, Deputy Director, Adams County (Colorado) Communication Center

TODD BIANCHI, Firefighter Paramedic, Washington, District of Columbia Fire and EMS Department

JIM KOHLER, Deputy Director, Enterprise Technology Services, Alaska Department of Administration, State of Alaska

BRENDA L. DECKER, Chief Information Officer, State of Nebraska

APPEARANCES: (Cont'd)

CHARLES L.K. ROBINSON, Director, Business Support Services, City of Charlotte, North Carolina

BOB AZZI, Senior Vice President, Network, Sprint Nextel Corporation

DIANE C. WESCHE, Director, Government Network and Technology, Verizon Wireless

ED CHAO, Senior Vice President, Corporate Engineering and Network Operations, MetroPCS Communications, Inc.

RON STRECKER, Chief Executive officer, Panhandle Telephone Cooperative, Inc., and Panhandle Telecommunications Systems, Inc.

KENNETH C. BUDKA, Senior Director, Advanced Mission-Critical Communications, Bell Labs Chief Technology Office, Alcatel-Lucent

DENNIS MARTINEZ, Chief Technology Officer, RF Communications Division, Harris Corporation

PAUL STEINBERG. Senior Vice President and Chief Technology Officer, Motorola Solutions, Inc.

PANEL 1: THE SCOPE OF RECOMMENDATIONS DEVELOPED BY THE INTEROPERABILITY BOARD

BRIAN FONTES, CEO, National Emergency Number Association

ANNA GOMEZ, Deputy Assistant Secretary for Communications and Information, National Telecommunications and Information Administration

ROBERT LEGRANDE, Advisor to the City of Baton Route, Louisiana

JEFF COHEN, Chief Counsel, Law and Policy Director of Government Relations, Association of Public Safety Communications Officials (APCO)

PANEL 2: STANDARDS, INTERFACES, GUIDELINES, USER EQUIPMENT, AND DEVICE MANAGEMENT; NETWORK EVOLUTION

TOM SORLEY, Chair, National Public Safety Telecommunications Council (NPSTC) Technology Committee

AJIT KAHADUWE, Head of Industry Environment, North America, Nokia Siemens Networks

PATRIK RINGQVIST, Vice President, Wireless Network Solutions, Ericsson

MARTIN DOLLY, Lead member of the Technical Staff, Core Network and Government Regulatory Standards AT&T

APPEARANCES: (Cont'd)

PANEL 3: MOBILITY AND HANDOVER; GRADE OF SERVICE; PRIORITIZATION AND QUALITY OF SERVICE

PAT AMODIO, Chief Engineer, DHS Joint Wireless Program Management Office, U.S. Customs and Border Protection
ROGER QUAYLE, Chief Technology Officer and Co-Founder, IP Wireless
ROBERT WILSON, Telecommunications Manager, Wyoming Department of Transportation, State of Wyoming
SCOTT C. SOMERS, Vice Mayor, Mesa City Council, City of Mesa, Arizona

PANEL 4: SECURITY

MARK ADAMS, Director, Principal Architect, Networks and Communications, Northrop Grumman
THOMAS FARLEY, Senior Systems Engineer, Network Centric Systems, Raytheon
MATT SCHNELL, Supervisor of Telecommunications, Nebraska Public Power
MARK ALTHOUSE, Technical Director, Mobility Mission Management, National Security Administration

1 P R O C E E D I N G S

2 (9:01 a.m.)

3 MR. BARNETT: Good morning and welcome, and thank
4 you all for being here. Chairman Chuck Robinson, I have
5 a few opening remarks, but a couple of housekeeping
6 things first.

7 It's great that you're here. We love having
8 guests here, but because of the way that our security
9 system is set up, it's very difficult for you to go to
10 the courtyard for coffee. No problem going to the
11 restrooms, which are just down the hall. But if you do
12 go to the courtyard, you'll need to be escorted by an FCC
13 employee, and someone over in this area right here can
14 help you coordinate that if you need to do that.

15 My name is Jamie Barnett, and for the last two
16 years and nine months I've been privileged to serve as
17 the Chief of the Public Safety and Homeland Security
18 Bureau of the FCC. As many of you know, I will leave
19 this post this coming Friday and return home to the
20 Potomac Institute for Policy Studies. I leave my duties
21 in the capable hands of David Furth, who will serve as
22 Acting Bureau Chief, and Deputy Bureau Chief Jennifer
23 Manor will continue to support the Interoperability
24 Board.

25 One of my distinct privileges as Bureau Chief was

1 to help impanel this Interoperability Board, a group of
2 extraordinarily gifted technical experts, and I got to
3 address them just four weeks ago as they embarked on a
4 statutorily imposed 60-day dash to develop minimum
5 technical interoperability requirements.
6 My remarks today are also addressed to the
7 Interoperability Board, though it's okay with me if the
8 rest of you listen in. The statute imposes a simply
9 stated but terribly difficult duty on the members of the
10 Interoperability Board to develop the new public safety
11 broadband network authority for FirstNet, a recommended
12 minimum technical requirements to ensure a nationwide
13 level of interoperability for the nationwide public
14 safety broadband network.
15 Now this is an exceptional once in a lifetime
16 opportunity to bake in interoperability into this new
17 network as it is being launched. For the last two years
18 and nine months that I can account for and longer than
19 that really, the FCC has focused on the technical
20 requirements for interoperability, and I've learned some
21 key principles about interoperability from direct
22 observation and I'd like to share them with you.
23 First, there is certainly no natural law of
24 interoperability. Indeed, it seems the laws of nature
25 pull away from interoperability. Market forces do not

1 promote interoperability, or we wouldn't have the problem
2 we do. American ingenuity promotes product
3 differentiation. That's what we do. We try to make
4 things better, but sometimes that pulls against it.
5 Second, there are very few paths by which you can
6 achieve interoperability but 1,000 ways to thwart it.
7 Third and probably most important since it builds
8 on the first two principles, interoperability must be the
9 first priority if it is to be achieved. Now I've learned
10 that interoperability is high on everyone's list, a top
11 five priority, but it is almost never anyone's top
12 priority, and whenever anything else takes precedence
13 over interoperability, interoperability just doesn't get
14 pushed down a little. It can be obliterated.
15 What can take precedence over interoperability?
16 Control of the network, costs of the network, a desire
17 for flexibility can. While much of the work that this
18 interoperability board has already done is absolutely
19 excellent, the question of putting interoperability first
20 is why I've been alarmed at some of the discussions I've
21 heard about.
22 I've heard it as a clear position stated by at
23 least one and perhaps others that your recommendations be
24 nonspecific and provide FirstNet with flexibility. Now
25 flexibility sounds good until you remember your statutory

1 duty, what the law imposes on you, that you are to
2 develop minimum technical requirements to ensure national
3 interoperability. Not the best technical requirements,
4 not the most technical requirements, not the ones that
5 you would think would be most effective, only the minimum
6 to ensure nationwide interoperability.
7 And my question is can you allow flexibility
8 below the minimum. Some suggest that it was the
9 legislative intent that interoperability should provide
10 FirstNet with flexibility. There are no reports, no
11 legislative history that indicate this, and such a
12 position contradicts the plain language of Senator
13 Rockefeller's excellent bill and the action of the
14 Congress.
15 The Act went into specific detail about how you
16 were to be constituted, how your Chair and Vice Chair
17 were to be selected, how your travel should be covered,
18 how long you should deliberate and specifically what you
19 were to deliver. It does not mention flexibility once in
20 regard to the Interoperability Board.
21 And you are technically oriented experts. You
22 know that the more specific you are the less chance there
23 is for doubt, confusion, miscalculation and even
24 deliberate misinterpretation. Technical requirements
25 must be expressed in technical terms with engineering

1 precision or they can be worthless. Platitudes cannot be
2 technical requirements. Renaming interoperability as
3 operability means nothing if jurisdictions cannot
4 communicate with each other.
5 Now, if you're interested in what the FCC thinks
6 the minimum should be, we have a memorandum in the docket
7 that's based on two years of work that Interoperability
8 asked us to provide. You don't have to accept any of it
9 or even part of it. That's the Board's choice. The FCC
10 is not in a position statutorily and will not impose the
11 memo on you. But I know that if FirstNet ends up with
12 interoperability problems, there may be a comparison of
13 that work against that memorandum.
14 Now I'm very happy that there will be a
15 nationwide public safety broadband network and that
16 billions of dollars will be invested to make it a
17 reality. But if it turns out that FirstNet is not
18 interoperable nationwide, the nation will look back at
19 the Interoperability Board and ask why. What will be
20 your answer? We wanted the network to have flexibility.
21 We didn't want to be too specific.
22 But your duty is and was interoperability,
23 interoperability first, the first priority. I thought
24 back over these years about 9/11 and the lives that we
25 lost and the ones among those that could be attributed to

1 the fact that we didn't have interoperability. And we've
2 had disasters and calamities since then where we had
3 lives lost because of interoperability and the lack of
4 it. Lives of civilians and lives of first responders,
5 first responders who were responding to their duty, and
6 really unfortunately we can't do anything for them now,
7 the ones that are gone.
8 Somewhere right now there's a young firefighter,
9 a policewoman, a deputy sheriff going on duty, suiting
10 up. We can do it for them so that they don't have to die
11 in the line of duty because we couldn't get lifesaving
12 information in the communications devices that were in
13 their hands.
14 Congress has given you a clear duty, minimum
15 technical requirements for interoperability. I know the
16 Board has the expertise. I know that you're up to the
17 task. I know you will do your duty.
18 Since my time here, I've had the pleasure of
19 working with the Department of Homeland Security's Office
20 of Emergency Communications and Chris Essid, its leader,
21 and he's here to speak with us next. Chris and his team
22 -- I'll add of them together -- have done an outstanding
23 job, comrade in arms for interoperability, they've done a
24 great job with the emergency -- come on up, Chris -- the
25 emergency communications preparedness center, with

1 SAFECOM, with any number of different projects. Chris,
2 it's been my pleasure to work with you, and I now turn
3 the rostrum over to you.
4 MR. ESSID: Thank you, Jim. Good morning and
5 welcome. Thank you, Admiral, for that kind introduction,
6 and before I move on, I wanted to thank Admiral Barnett
7 for all of his efforts in his current role. You know,
8 he's going to be departing soon and our partnership with
9 the FCC, and Admiral Barnett has been an outstanding one,
10 and so thank you for everything you've done for
11 interoperability, for public safety emergency
12 communications, and I wish you the best in all your
13 future endeavors.
14 (Applause.)
15 MR. ESSID: Well deserved. Well deserved.
16 Well, the Office of Emergency Communications was
17 created by Congress to address some of the communications
18 issues the nation experienced on 9/11 and during the
19 response to Hurricane Katrina. The mission Congress gave
20 our small little office is fairly straightforward: to
21 ensure that emergency responders and government officials
22 can communicate in day-to-day situations and also during
23 disasters.
24 We accomplish this mission by engaging in and
25 collaborating with our federal, state, local and public

1 safety stakeholders and partners. These are our
2 customers. This stakeholder engagement is the mission
3 and is one of our many reasons that the Office of
4 Emergency Communications is named in the law that brought
5 us here today. This is so critical. NYOEC will
6 represent DHS in these efforts as we move forward toward
7 implementing this nationwide public safety broadband
8 network that we're here to discuss.
9 Many of the people in this very room fought long
10 and hard to get us where we are today. It was a
11 difficult battle and we had many setbacks along the way.
12 But the public safety community persevered to see one of
13 the last outstanding recommendations of the 9/11
14 Commission become closer to reality, and that's
15 establishing a nationwide interoperable public safety
16 network.
17 A nationwide public safety broadband network must
18 be built to support the needs of its users at all levels.
19 This is one of the reasons why starting with the
20 creation of this interoperability board the work to see
21 this initiative succeed has entered a brand new phase.
22 While much of the initial work to stand up the network
23 will take place inside the beltway, the involvement of
24 all the stakeholders are going to be key to ensuring the
25 success of this network.

1 The input, feedback and involvement of police
2 chiefs, fire chiefs, mayors, governors, communications
3 personnel like we have here today in the room is going to
4 be vital to developing and deploying this network and to
5 make it a success.
6 OEC will continue to collect this input through
7 our existing stakeholder groups like SAFECOM where public
8 safety and government officials are represented and have
9 an opportunity to provide advice and recommendations to
10 the Department of Homeland Security and federal
11 government.
12 Additionally, we're going to use groups like the
13 National Public Safety Telecommunications Council or
14 NPSTC to coordinate a lot of things as well. You know,
15 working together, we're going to be successful. That's
16 how we got here.
17 As you know, OEC does a lot of work also
18 coordinating federal emergency communications efforts.
19 Since the law provides access to federal first
20 responders, this is a real opportunity to improve
21 interoperability amongst all levels of government --
22 federal, state, local, tribal -- responders to ensure
23 that communications capabilities can be achieved that
24 we've never had before.
25 Later today you're going to hear from a

1 representative of the DHS Joint Program Office, dedicated
2 to providing next generation communications to DHS's
3 first responder community. DHS has been coordinating our
4 internal DHS efforts through a group called the One DHS
5 Emergency Communications Committee, and we've made
6 significant progress by developing a strategy and more
7 recently collecting broadband requirements from our first
8 responders at the federal level.
9 As you'll remember, not too long ago DHS was
10 created and a lot of different groups were put together
11 and a lot of different groups with public safety
12 missions. So we're coordinating like never before within
13 our own department. Bringing federal first responders
14 and all the resources to the table will be a challenge,
15 but we'll make sure this effort is coordinated by doing
16 things we always have done, and that's direct engagement
17 with all the stakeholder community to make sure we do it
18 right.
19 It's essential that this network is inherently
20 interoperable, and the only way to ensure that is by
21 soliciting input from all of our stakeholders. I
22 understand that the board has been working at a furious
23 pace with a commitment to develop minimum requirements
24 and provide FirstNet with the information necessary to
25 start the RFP process. What the Board has done and what

1 we do here today, in the coming weeks, in the coming
2 months, will establish a foundation to achieve a goal
3 that previously seemed beyond our reach.
4 I'd like to thank the Interoperability Board
5 members for their time and their dedication over the past
6 few weeks, what you've done and what you're about to do.
7 I'd also like to thank our audience for
8 participating today, and as always, if there's anything
9 the Office of Emergency Communications or DHS can do,
10 please reach out to us. We look forward to working with
11 everyone as we take these next steps to make this network
12 a reality. Thank you.
13 (Applause.)
14 CHAIRMAN ROBINSON: Good morning. My name is
15 Chuck Robinson, and I am the Chairman of the
16 Interoperability Advisory Committee. Excuse me, Advisory
17 Board. And I have to say this is something of a great
18 big pleasure for me and also a very daunting task. I
19 never would have anticipated a few months ago that I
20 would be sitting where I am right now and having been
21 selected by such a distinguished group of folks to be
22 their chairman.
23 It's a little frightening, but at the same time,
24 I'm having the time of my life, and I'm enjoying this
25 very, very much. It's very rare that you get to work

1 with such a distinguished and great team of professionals
2 in trying to do something positive, a first time record-
3 setting for public safety in this country.
4 I want to thank Jamie Barnett for his remarks and
5 for his contributions to the future of American public
6 safety as the Bureau Chief of the Federal Communications
7 Commission Bureau of Public Safety and Homeland Security.
8 We all wish him the very best as he transitions into a
9 new but familiar role. We also want to say welcome to
10 David Furth in his new role and look forward to working
11 with him as the Board completes its work.
12 I also want to thank Chris Essid for his remarks
13 and the great support that the Department of Homeland
14 Security Office of Emergency Communications has been
15 throughout this entire effort not only in the work that
16 they've done through SAFECOM and technical assistance
17 programs that have been a big help to state and local
18 agencies as they tackle the issues of public safety
19 communications and interoperability but in the many
20 little ways that they have helped those of us who are
21 trying to deploy broadband networks now.
22 As you've heard from the remarks, there's an
23 intense amount of pressure on this Board to deliver a
24 high quality product in a very short amount of time, and
25 I have to say I'm impressed by the Board Members' work,

1 their commitment to this process. Hours and hours a week
2 are being poured into this while everybody else I know
3 has full plates as we move through this process.
4 It's a daunting task. It's a balancing act. How
5 do we ensure nationwide interoperability at the same time
6 that we look at how states and local jurisdictions deploy
7 these networks, use these networks and ensure these
8 networks work for those who are on the ground and need
9 the service in an emergency.
10 I want to now introduce the Board Members to you.
11 First, I'll start to my right. Ken Budka, who is our
12 Vice Chairman from Alcatel-Lucent; Paul Steinberg, who is
13 a Subcommittee Chairman and with Motorola Solutions,
14 Incorporated. And then Brian Shepherd from Adams County
15 Communications Center in Colorado, a fellow local
16 jurisdiction developer. I also want to introduce Dennis
17 Martinez, who is Subcommittee Chair for our Drafting
18 Committee, who's done a very good job of helping us frame
19 the document that will be coming forward. Bob Azzi from
20 Sprint Nextel.
21 If you would just raise your hands so folks get a
22 shot at who you are. Thank you. Todd Bianchi from the
23 Washington, D.C. Fire and EMS Department. Ed Chao, who
24 is not with us this morning. Ed, are you on the line?
25 Do we have a conference line up? It is up? Okay. Well,

1 Ed will be listening in today. Brenda Decker from the
2 State of Nebraska. Ken Hughes from the New Orleans --
3 and I hope I said that right. You know, there's an art
4 to saying New Orleans, from the Urban Area Security
5 Initiative. Ken, are you on the line?
6 MR. HUGHES: I am, and you said it correct.
7 CHAIRMAN BARNETT: Okay. Thank you very much. I
8 practiced that. And Bill Price from the State of Florida
9 Division of Telecommunications. Steve Proctor from the
10 Utah Communications Agency network and then Ron Strecker
11 from Panhandle Telephone Cooperative, Incorporated and
12 Diane Wesche from Verizon Wireless.
13 I believe everybody knows why we're here today.
14 The workshop will consist of four panels. I'm really
15 messing up today. I forgot to mention Dereck Orr from
16 NIST as well. Dereck, my apologies. I've got it all
17 laid out here and I can't read what I've written. I'll
18 get over this.
19 As I believe everybody knows, today our workshop
20 consists of four panels. Each panel has four speakers.
21 Each speaker will have seven minutes to present their
22 prepared remarks. After all four speakers have presented
23 their remarks, the moderator will open the session for
24 questions. The moderator will ask questions of board
25 members first. After each board member has been given an

1 opportunity to ask a question, then the moderator will
2 take questions from the audience.
3 After the audience has asked their questions, the
4 board members will be given a second opportunity for
5 questions, and then the board moderator will go back to
6 the audience and we'll continue in that way until all the
7 time has expired.
8 There will be a 15-minute break between the
9 second and third panels, which should happen right around
10 11:00. And with that, I think my opening remarks are
11 finished, and we may get to the first panel early, which
12 would be a good thing. So let me start out. We aren't
13 going to go through the bios. Those are inside of your
14 program. We'll simply be introducing the speakers and
15 the organizations that they represent.
16 So it's my pleasure to start by introducing Mr.
17 Jeff Cohen, who is Chief Counsel with the Association of
18 Public Safety Communications Officials, and Jeff, we're
19 happy to hear from you.
20 MR. COHEN: So let me begin with a short roadmap
21 of what I'll be presenting today. The starting point is
22 the text of the legislation, which directly speaks as
23 Admiral Barnett had mentioned in his opening remarks to
24 the scope of the Board. Then I'm going to talk about
25 some governing principles that the Board should follow,

1 consistent with the public safety legislation generally,
2 and finally I'll provide some high level feedback on the
3 scope of the recommendations that the Board had produced.
4 The first slide is just a repeat of the standards
5 as I understand, I'm sorry, the scope of the work as I
6 understand that the Board has introduced. Public safety
7 legislation, as again Admiral Barnett had said, the
8 legislation is very brief on the subject and it's
9 intended to address the scope of the Board, and each word
10 has meaning. The Admiral stepped it through, I'll do it
11 again, develop recommended minimum technical requirements
12 to ensure nationwide level of interoperability.
13 So the whole purpose of the Board's
14 recommendations is to ensure a nationwide level of
15 interoperability, which of course is the goal at the
16 heart of the legislation that was just enacted.
17 The second and only other point where the
18 legislation gets into specifics is it says that the Board
19 shall base its minimum recommendations on the commercial
20 standards for long-term evolution.
21 The commercial standards itself is a defined term
22 in the statute. It means the technical standards
23 followed by the commercial mobile service and commercial
24 mobile data service industries for network, device and
25 internet protocol connectivity. The definition

1 references the standards developed by 3GPP, IEEE, ATIS,
2 IETF and ITU, and importantly this term, commercial
3 standards, is later used in the definition in the
4 legislation of the public safety broadband network
5 itself. In fact, it is here where FirstNet is made
6 solely responsible for ensuring the establishment of the
7 network. The two defined network components in the
8 statute, the core network and the radio axis networks,
9 are to be based on commercial standards.
10 This is why I say in my last bullet on this slide
11 that it's important to keep in mind when understanding
12 the scope of the Board that Congress vested solely with
13 FirstNet broad and significant responsibilities. It is
14 to ensure the establishment of the network and conduct an
15 open and transparent RFP process where FirstNet is to
16 identify and include the technical and operational
17 requirements of the network, among many other
18 responsibilities.
19 Importantly, FirstNet is also required to
20 incorporate the input from the state and local planning
21 process. With that said, I just want to present a few
22 governing principles that are consistent with the
23 specific direction of the statute for this Board and also
24 with the responsibilities of FirstNet.
25 First, as I've already discussed, adherence to

1 commercial standards should be a guiding principle.
2 Second, whatever recommendations are developed should
3 help enable FirstNet to maximize opportunities for
4 public-private partnerships. Also, we should try to
5 ensure a robust RFP response. Let's remember that the
6 recommendations the Board comes up with get incorporated
7 into the RFPs. It's then up to the response from the
8 community that's responding to the RFPs whether or not
9 they'll be able to meet these requirements.
10 Also, we would suggest that the recommendations
11 foster a competitive and diverse vendor environment, that
12 it anticipates advances in technology. Of course, this
13 is a dynamic technology, LTE. I don't pretend to speak
14 to it technically, but we know that it grows by leaps and
15 bounds, especially with its new releases.
16 Also, we look to seek to preclude proprietary
17 implementations and applications that would interfere
18 with achieving and maintaining interoperability, and
19 finally, account for roaming agreements with commercial
20 providers, which is the responsibility of FirstNet to try
21 to achieve.
22 I'll next address briefly a summary action from
23 APCO, including its broadband committee, on some of the
24 Board's defined scope. First, on the standards,
25 interfaces and guidelines, one question that we would

1 pose to the Board is how is vendor level interoperability
2 achieved or not in the commercial LTE marketplace today
3 and what gaps would need to be filled.
4 On user equipment and device management, other
5 than type acceptance, the legislation directs NIST to
6 develop a list of certified devices and components. Are
7 there any gaps here?
8 On network evolution, we should account for
9 FirstNet discretion concerning implementation of new
10 releases, and finally on mobility -- sorry, not finally,
11 but on mobility and handover, we need to support network-
12 to-network LTE handovers.
13 Grade of service priority, prioritization and
14 quality of service, we view that there are two levels of
15 network management: the physical network, which is under
16 the purview of FirstNet, and then operational control,
17 which could be enabled by FirstNet to permit local
18 changes to priority and quality service on a fluid and
19 incident-by-incident basis.
20 Finally, on security, we believe that we need
21 multiple layers of network and application security.
22 Access to the public internet should be available but
23 limited and quickly disabled if needed. And I would just
24 point out that the legislation includes national security
25 restrictions and requires network safety security and

1 resiliency in the design of the network. And with that,
2 I'll turn it back to you, Chuck. Thank you.
3 CHAIRMAN ROBINSON: Thank you very much. Great
4 timing.
5 MR. COHEN: Well practiced.
6 CHAIRMAN ROBINSON: I appreciate that very much.
7 We'll now move on to our second speaker, Brian Fontes,
8 who is the CEO of the National Emergency Numbering
9 Association. Brian.
10 MR. FONTES: Thank you. I appreciate the
11 opportunity to be here this morning, and thank you for
12 the invitation to be on this panel. I'd like to just
13 first introduce who NENA is. NENA is an organization
14 that represents the 911 community. In large part, it's
15 the organization that has been primarily responsible for
16 developing standards and services in the 911 field. We
17 are very much involved in the education and training of
18 the 911 professionals across the country.
19 Before I begin, there are three things that I'd
20 really like to convey in the short time that I have with
21 you this morning. One is how Americans communicate and
22 what the expectations of consumers are. Secondly, what
23 the statute says with respect to integrating 911 or
24 public safety answering points with FirstNet and the
25 third point is to give you a little bit of information

1 about next generation 911. And so I would like to begin
2 by showing this little edgy video here, and this pretty
3 much describes how the public communicates. Hopefully
4 this will work.
5 (Video presentation.)
6 MR. FONTES: What I want to try to do in this is
7 this is just simply the expectations that the consuming
8 public has in today's world. They communicate in voice
9 video and data. In today's 911 world, we're moving from
10 the voicecentric environment to an information-rich voice
11 video and data environment.
12 So, when we talk about the interoperability
13 aspects of this, I'm going to skip to what the statute is
14 saying, the statute says basically that FirstNet shall
15 promote the integration of the network with the public
16 safety answering points or their equivalent.
17 So it's in the law basically that there has to be
18 the integration of the PSAP and FirstNet's services. So
19 I think that it's critically important to understand that
20 there are other facets of the law that Jeff indicated,
21 and I have these in the slides here.
22 But what's driving all of this? With respect to
23 next generation 911, we need to mainstream 911
24 technologies into the 21st century. We need to have
25 improvements for survivability, and we need to improve

1 the interoperability and information sharing that will be
2 necessary in this 21st century way of communicating.
3 The desire to increase competition in innovation
4 is simply there. Next generation 911, trying to connect
5 with the slides here, is an open standards based platform
6 using modem, flat IP architecture with robust security
7 and resilient features. It's based on commercial off-
8 the-shelf technology, and it's designed to be an
9 originating service agnostic capability. Text 911 and
10 instant messaging is critically important.
11 Files to 911, such as photos and clips, are just
12 part of the way people communicate today. Streaming
13 video, likewise. Telematics and sensors will become an
14 increasingly important element in the provision of
15 security and information coming into the 911 centers.
16 Nomadic and/or mobile call-taker workstations
17 will become a reality in the next generation 911
18 environment. When we talk about next generation 911, it
19 talks about allowing seamless flow of data from consumers
20 to call-takers to dispatchers to those who will be
21 responding utilizing FirstNet. It leverages existing
22 national standards for interfaces and data structures.
23 It provides an adaptable platform to meet future
24 responders' needs.
25 In this rich information world that we live in

1 today, roughly 900,000 911 calls are made each day, and
2 when you think of the world that we live in, with 330
3 million wireless devices, with a population of 313
4 million, most of that communication is non-voice
5 communication. Two-thirds of it in fact is non-voice
6 communication. And it is that capability of connecting
7 with a 911 center and having that 911 center integrate
8 and interoperable with FirstNet will provide the public
9 with the best service available. Thank you.
10 CHAIRMAN ROBINSON: Thank you. And now we will
11 move on to Ms. Anna Gomez, who's the Deputy Assistant
12 Secretary for Communications and Information. Anna,
13 thank you so much for coming this morning.
14 MS. GOMEZ: Thank you very much, Chuck. Let me
15 join everybody who has expressed their best wishes to
16 Admiral Barnett. He has been a great advocate for public
17 safety and really a pleasure to work with in this
18 Administration. So best wishes. I look forward to
19 seeing you in your next iteration.
20 I'm delighted to be here at this workshop, and by
21 the way, thank you, Chuck, for inviting me, and thank you
22 to the Interoperability Board for having us here. So
23 this workshop is on interoperability, which is a key
24 impetus to the new law establishing the new single
25 nationwide interoperable public safety broadband network.

1 And the new network certainly will bring public safety
2 into the broadband age and will bring valuable new
3 applications like building maps for firefighters who are
4 battling a blaze or license plate lookups for the police
5 who are approaching a suspect, many other lifesaving
6 applications that I won't go into because I only have
7 seven minutes. But these new applications will mean
8 precious little if the firefighters can't in fact
9 communicate with the police in an incident.
10 So we're all grateful for the work that this
11 very, very hard-working board is doing to provide a
12 foundation for interoperability of the single nationwide
13 broadband network for public safety. Multitasking, we're
14 supposed to be good at that, but I don't know. We'll
15 see.
16 Anyway, the new law makes good on an overdue
17 promise to first responders, the chief of which is to
18 ensure this single nationwide public safety broadband
19 network which is based on a single national network
20 architecture.
21 And the topic of today's panel is scope, so I
22 thought I'd go back to the basics, much like both Brian
23 and Jeff have done, and that is to the words of the
24 statute and to sketch for you what the law says about the
25 minimum technical requirements you have been tasked in

1 formulating in this very brisk timeframe. But first I
2 want to mention the first responder network authority or
3 FirstNet. It has been mentioned already, but I want to
4 make sure that we talk about this first.
5 The Act establishes FirstNet as an independent
6 authority within NTIA, which is required to build,
7 operate and run this network, and here are just some of
8 the duties that FirstNet must carry out in building and
9 deploying this network.
10 Minimum requirements are a critical baseline, but
11 this new startup network operator must meet these and
12 then do a whole lot more. Some of these responsibilities
13 include leveraging commercial infrastructure to the
14 maximum extent economically feasible; ensuring against
15 cyber attacks; promoting competition in the equipment
16 market and including substantial rural milestones in its
17 deployment plans, and this is just a partial listing of
18 what FirstNet has been tasked with doing
19 This is also kind of going back to basics, but
20 the FirstNet Board, with three federal and 12 non-federal
21 members, have also mandatory public safety as well as
22 state and local representation. And the reason that I'm
23 going through this is because this is an entrepreneurial
24 operational board. It is a board of real experts,
25 experts in public safety, technical gurus, real network

1 managers and real financial wizards. It must be
2 entrepreneurial in spirit to accomplish the build of a
3 single cutting-edge network that will meet the unique
4 demands of public safety, and it must also be able to
5 update and revise its network policies as it maintains,
6 operates and improves this network, the nationwide public
7 safety broadband network.
8 And as I know you are all aware, the Act sets
9 forth some very tight deadlines, and it's significant
10 that right out of the box the law focuses the Commission
11 and the technical advisory board on interoperability. So
12 your diligent work is going to factor into the requests
13 for proposals that the private sector will answer for
14 building, operating and maintaining that network.
15 Now, for folks who are interested in the state
16 opt-out process, I do list here some of the statute's
17 provisions with regard to opt-out, and why this is
18 relevant is because the statutory language limits the
19 opt-out bill to the radio access network and does not
20 include the evolved packet core. But as you know, the
21 FCC will take the minimum technical operability
22 requirements you recommend into account as it reviews and
23 passes on the state opt-out plans. It will also take
24 into account interoperability with the nationwide
25 network.

1 Once the FCC is done and if it approves the plan,
2 then NTIA must review the state opt-out plans according
3 to several criteria before it either awards a grant to
4 build a radio access network, or I shouldn't say either,
5 and before it permits a lease of the spectrum from
6 FirstNet.
7 So these criteria include the technical and
8 financial capabilities to support the state radio access
9 network, the ability to maintain ongoing interoperability
10 with the public safety broadband network, the ability to
11 complete the project within timelines comparable to
12 FirstNet's plan for the state and with comparable
13 security, coverage and quality of service to the public
14 safety broadband network. And the state must show to
15 NTIA that its plan is cost-effective.
16 So that was basically the baseline that I wanted
17 to talk to you about. Your work, we view it as a
18 constitution. It's a set of baseline requirements. But
19 we urge you to resist the urge to stand in FirstNet's
20 place in developing the network architecture and its
21 business and operational plans. FirstNet must be able to
22 respond in a nimble fashion to changes and improvements
23 in technology.
24 Admiral Barnett talked about the network not
25 having flexibility that thwarts interoperability, but I

1 will tell you FirstNet must have the flexibility to be
2 able to operate and maintain this network over the years
3 to come. Your work is very important as the baseline for
4 interoperability requirements, and we really look forward
5 to continuing to work with you and continuing to see how
6 hard you are working to develop that exact plan so that
7 the network can succeed for public safety. Thank you
8 very much.
9 CHAIRMAN ROBINSON: Thank you, Anna. I
10 appreciate that very much.
11 Our next speaker is actually on the telephone,
12 Mr. Robert LeGrande, who is the President and CEO of
13 Digital Decision, who is here today -- well, not here
14 today, but is representing the City of Baton Rouge,
15 Louisiana. Robert was at the APCO conference and
16 unfortunately had some passport issues. I think his
17 passport got stolen, and so he's been unable to return to
18 the United States and is joining us by phone. Robert,
19 are you there?
20 (Discussion held off the record.)
21 CHAIRMAN ROBINSON: Okay. Well, Robert evidently
22 is not on the line, so I guess at this point we'll go
23 ahead and open for questions, and if Robert joins us
24 later on, we will move forward with his comments.
25 All right. Thank you. So, as I mentioned

1 earlier, the first thing that we're going to do is to
2 open questions to the Members of the Interoperability
3 Advisory Board, and so with that, I would ask the panel
4 here are there any questions for any of our speakers?
5 VICE CHAIRMAN BUDKA: We spoke and Admiral
6 Barnett gave us some advice at the beginning of today's
7 session about the tension between setting specific
8 requirements and also flexibility, particularly in
9 regards to picking particular commercial standards, for
10 example, device management and things like that. I
11 wonder if you have any advice for the Board as we try to
12 wrestle with picking specific requirements that can be
13 used to ensure interoperability but also providing some
14 level of flexibility that may be needed operationally as
15 FirstNet goes forward. I'd open that up to all the
16 panelists.
17 MR. COHEN: So the process is going to be an RFP-
18 based endeavor by FirstNet, and the commercial industry
19 hopefully will respond and probably respond in ways that
20 will reflect the way that the commercial industry today
21 is deploying LTE networks, whether it's service providers
22 or the manufacturers. So my best advice and response is
23 to keep in mind that the recommendations you're
24 developing that will go into these RFPs should reflect as
25 best as possible the ways that commercial service

1 providers are deploying but of course with the knowledge
2 that this is a network specific for public safety.
3 But we need to try to enable FirstNet to achieve
4 economies of scale and scope and national bargaining
5 level power on behalf of public safety that they have
6 never been able to achieve to date. So I hope that's
7 helpful.
8 MR. FONTES: Yes, I think Jeff summed it up. I
9 think the important thing is to have that appropriate
10 balance between what is absolutely essential for the
11 network to work and to be interoperable and to ensure
12 that you do not become so defined in the functionality of
13 it that the likelihood of bidders to respond to the RFP
14 would in fact be small.
15 And I think that what we have to recognize is the
16 important aspect of any type of commercial technology, in
17 this case LTE, is that you want to make sure that that
18 first network is always refreshed and that you have to
19 make sure that the interoperable requirements are to that
20 threshold that would allow for that type of refreshing
21 rather than actually rebuilding. So I think that's
22 critically important.
23 MS. GOMEZ: I don't think I can add anything
24 more. I'm sorry. That was exactly on point.
25 MR. STEINBERG: Thank you very much for being

1 here and for your excellent remarks. One question I had,
2 and Jeff, I think you kind of reviewed our scope or at
3 least as we currently envision it, flipping the question
4 around, what, if anything, do you see that we might be
5 missing? Is there anything we're not considering that we
6 should be?
7 MR. FONTES: Well, I'll start this out. First
8 off, to try to define what you're missing, I would have
9 to know what it is that you have already considered, and
10 I don't. And so I'm sure that a lot of the work is being
11 developed and reviewed internally at this point, and I
12 respect that.
13 But one of the things, I think that there is a
14 lot to be learned from history, and I think that as you
15 go back and you take a look at the whole evolution of
16 trying to create a public safety wireless broadband
17 network is in the complex tug-of-war if you will between
18 what is necessary for the provisioning of public safety
19 services and what is minimal for the provision of public
20 safety services there's kind of the wish list and the
21 reality, and oftentimes the wish list kind of gets the
22 heavier weight if you will on the scale, and as a result
23 of that, you may in fact be developing a set of criteria
24 that provides a disincentive rather than an incentive to
25 build that network.

1 And the first tranche of this going out, I mean,
2 we will learn a lot, and I think that both from the
3 public safety perspective and the commercial perspective
4 there will have to be additional fine-tuning of the
5 requirements.
6 And the video that I presented here has so many
7 applications with all due respect to the public safety
8 broadband network, because I think so often we think in
9 the world that we're in 10 years ago or were in 10 years
10 ago and the world that we're in now, and I envision a
11 public safety broadband network capable of providing
12 applications developed by and for public safety, whether
13 it's for the unique location of New York City -- I met
14 somebody here from New York City earlier -- or from some
15 of the other municipalities -- that may be an application
16 unique to that community.
17 Yet it's still riding that public safety wireless
18 broadband network, and so I think that we have to make
19 sure that the needs of public safety are met in a manner
20 that will allow and invite as many participants in the
21 development of the technology that will be riding that
22 network.
23 CHAIRMAN ROBINSON: Thank you.
24 MR. COHEN: Just one real quick point too. Maybe
25 it could have been included among what I subtermed

1 governing principles, but another important consideration
2 I think is to remember how much federal money is actually
3 allowed for this, $7 billion. Seven billion is a lot of
4 money, but it's also not a lot of money. So I'd suggest
5 that you consider what that can accomplish and what it
6 should and then what add-ons after that we could do, but
7 focus primarily on where the federal money should best be
8 used. Thanks.
9 MS. GOMEZ: Yes. Again I'd echo my fellow
10 panelists here. So looking at the working concept of
11 scope and definition that the Board has already put
12 together, I would say we agree with it. It focuses on
13 the interfaces and the protocols between the systems and
14 the system components, and the only other thing I would
15 urge is to focus on what FirstNet needs to do, not how it
16 should do it as you put this together. But beyond that,
17 that's about as much advice as I can give.
18 CHAIRMAN ROBINSON: Before we move on to the next
19 question, I want to check one more time to see if Robert
20 LeGrande is on the phone.
21 (Discussion held off the record.)
22 MR. FONTES: Charles, I just read his email last
23 night. He said that he would try to be on the call, but
24 if he was at the consulate, he wouldn't be able to make
25 it.

1 CHAIRMAN ROBINSON: Right. I understand. Yes,
2 Dennis, do you have a question?
3 MR. MARTINEZ: The statutes are silent on the
4 issue or topic of waiver assistance. Can you offer the
5 Board any insight into what we consider to be an
6 important part of the evolution of this network?
7 MS. GOMEZ: What specifically are you asking, I'm
8 sorry, with regard to the waiver recipients?
9 MR. MARTINEZ: Any insight. Given that the
10 statute is silent, the question is naturally asked what
11 ramifications are there to the scope of the Board's work?
12 MS. GOMEZ: Okay. Sorry. Thank you.
13 MR. MARTINEZ: It's a scope question.
14 MS. GOMEZ: Well, what I would say is the waiver
15 recipients and those that have been doing early build,
16 we're very proud of the work that they have accomplished.
17 It is important and there are important lessons learned
18 in what they have done.
19 FirstNet, however, needs to put together its
20 single nationwide architecture that best accomplishes the
21 objectives of having a nationwide public safety broadband
22 network that meets the needs of its users, that fits
23 within its budgetary constraints.
24 So while it can learn some very important lessons
25 from the early builders, I think the important thing is

1 to put yourselves in their place as they do the best
2 possible job from the beginning, meaning the minimum
3 technical requirements should take into account that this
4 is a single nationwide architecture, and sure, you can
5 learn lessons from it, but it should begin from the point
6 of view of FirstNet, which is they're going to come up
7 with the best business plan and the best architecture
8 that they can from scratch I would say.
9 CHAIRMAN ROBINSON: Thank you.
10 MS. GOMEZ: Now FirstNet will -- because I know
11 what you guys are all thinking, obviously FirstNet is
12 going to have to take into consideration what is out
13 there now as it moves on with its business and
14 architecture plan. And it's going to have to look at
15 what existing architecture there is from the commercial
16 perspective, what existing architecture there is from a
17 public safety perspective, what existing architecture
18 there is from a state and local perspective as well.
19 All of that becomes a part of the development of
20 its business plan and eventually the best plan for its
21 users, which is the public safety community.
22 CHAIRMAN ROBINSON: Thank you. Any other
23 questions from board members? Yes, Paul.
24 MR. STEINBERG: Anna, you talked a lot about
25 entrepreneurship. Where in government is there a current

1 model of entrepreneurship that FirstNet can follow so we
2 don't get $200 user devices and $3,000 toilet seats and
3 that kind of an issue?
4 MS. GOMEZ: You know, honestly off the top of my
5 head, I can't think of a business model. I will say that
6 at NTIA we are quite used to standing up new programs.
7 You know, the digital television coupon program for the
8 digital transition, our VTOT grants have been quite
9 entrepreneurial. And it takes a lot of oversight over
10 your functions and your procurement to ensure that in
11 fact you get the best value for taxpayers. So we are
12 committed to that type of outcome, and we will do
13 whatever we can to help FirstNet oversee its purchases
14 and its transactions and as it builds out its network to
15 ensure the best value for taxpayers.
16 MR. FONTES: I'd just like to add one thing to
17 that. Steve, I know you have another question. I think
18 the world is full of entrepreneurs, but there are fewer
19 successful entrepreneurs. And so you have to go back and
20 try to examine what contributes to the success of an
21 entrepreneurial activity, and the success of the
22 entrepreneurial activity will be the availability of
23 product and the acceptance of the product, which then
24 means the product is going to have to be priced and all
25 of the other aspects associated with that.

1 But you asked Anna a question, and from what I am
2 aware of, and you can speak best to this, but I think,
3 Jeff, when you asked the question, Jeff immediately said
4 Utah. What you have been able to achieve in Utah has
5 been pretty successful, and with all due respect, it's a
6 great model. You asked where there is a model, there's a
7 model right there in terms of involving communities,
8 involving the idea of developing and deploying equipment
9 that's readily available, that you're not paying
10 exorbitant prices for, that you benefit from the
11 competitive market in the purchasing of your equipment.
12 MR. PROCTOR: Thank you, Brian. It says --
13 CHAIRMAN ROBINSON: Steve, we're going to work
14 one question from the Board, and then we'll loop back
15 around. Is there another question from a board member?
16 Bob Azzi.
17 MR. AZZI: A question for any of you. In our
18 work, we've been using some reference documents from
19 other bodies of work that were related and came before.
20 I'm interested in knowing any particular areas that you
21 would point to bodies of work related in
22 interoperability, security, et cetera, that you'd like to
23 see the Board consider. One of the areas was CSRIC.
24 There's been a lot of work in cybersecurity and next
25 generation 911, et cetera. So I'd be interested in what

1 you'd like to at least see us look at and consider as we
2 go through this work.
3 MR. FONTES: Sure. First I'll start out. I
4 think that I appreciate the fact you're looking at what's
5 available out there across the board in any organization
6 that's developing standards.
7 From the next generation 911 perspective, clearly
8 the CSRIC efforts in identifying the standards work
9 that's been done, what needs to be done, et cetera, is
10 very useful.
11 The NENA i3 standard is being used a lot with the
12 CSRIC report in some of the FCC proceedings and so forth.
13 And so that's clearly an area where I would take a look
14 and say, okay, here is what's being developed dealing
15 with next generation 911 and how do we now incorporate
16 that or interface that with FirstNet to allow for that
17 true interoperability in the seamless movement of data
18 and information from the consumer to the 911 center to
19 FirstNet.
20 Any other standards work that's been done, I know
21 that when we went about and discussed the public safety
22 network, what, four years ago, if that, I mean, there was
23 a lot of unknowns at that time and it became very
24 disheartening to try to achieve a public safety broadband
25 network then. But I think what the statute has done is

1 try to eliminate a lot of that uncertainty by taking a
2 look at LTE technology, and that's the base for that
3 FirstNet network.
4 Now, for those in the wireless world, knows that
5 there are various flavors of LTE, but nonetheless it's
6 LTE. And so I think that we'll have an opportunity to
7 benefit from some of that standards work that has been
8 already developed and put into place. So I don't know of
9 any other standards work, you know, and I don't focus all
10 of my attention on standards bodies beyond just the 911
11 world, so I don't know.
12 MS. GOMEZ: What I would say is the statute does
13 direct the Board to work in consultation with NTIA, NPSTC
14 and the Office of Emergency Communications. I would urge
15 the Board to avail itself of the resources that you have.
16 The Office of Emergency Communications is a
17 wonderful resource to reach into a lot of the DHS work on
18 cybersecurity, for example, security issues. You're very
19 fortunate to have Dereck Orr as a technical expert, but
20 certainly NIST and NTIA through the Public Safety
21 Communications Research Program has a lot of information
22 they can provide and a lot of input.
23 So I would urge you to use that consultation in
24 maximizing as much as possible. Also NPSTC is a very
25 good resource for the Board. I'm sure you've already

1 considered it, but that's another suggestion.
2 CHAIRMAN ROBINSON: Thank you. Yes, Diane.
3 MS. WESCHE: Thanks, Bob. Diane Wesche. A
4 question for you. Ms. Gomez, you mentioned in your
5 remarks that we should resist the urge to kind of get
6 into more FirstNet's business. Those are my words, maybe
7 yours. So do you each have an example of something that
8 you think would cross the line that if we would weigh in
9 on and we would deliberate on that would be out of the
10 scope as you see, an example of something you really hope
11 that we do incorporate in our recommendations as the
12 Board tries to wrestle with what is our boundaries and
13 works within that and doesn't step over?
14 MS. GOMEZ: It's hard for me to come up with
15 specific ideas just off the cuff. I mean, what we're
16 looking at is minimum technical requirements. I would
17 really hate to see the Board delve into something that's
18 more of a business or an operational type of decision.
19 But maybe if I can let Brian and Jeff speak, I'll come up
20 with something.
21 MR. COHEN: Well, one thing is limit it to
22 technical aspects of interoperability. Of course there's
23 many other aspects of interoperability. In fact, that's
24 one of the reasons why there is a single national
25 governance body, because that's supposed to handle many

1 of the other -- actually all the aspects of
2 interoperability, but that including.
3 And then I'd just go back to one of my points on
4 one of my slides, to just keep in mind that these are to
5 be developed through the RFPs. So you, especially your
6 company is familiar with the industry and how it's
7 deploying, and so I would just recommend that you don't
8 go too far or include things that would preclude as
9 robust RFP response as is appropriate for this kind of a
10 network.
11 MR. FONTES: Well, I wish I had the answer to
12 your question because it's such an important question. I
13 mean, you can overspecify the requirements if you will of
14 a network, and in doing so, to Jeff's point, you're going
15 to just simply drive down the number of people who
16 respond and ultimately drive up the costs of the network
17 itself and everything that rides that network.
18 I think a lot of it should be looked at in terms
19 of interoperability, what is absolutely essential for
20 interoperability. I think the security issue is
21 critically important. In the world of application
22 development, I think there has to be some type of a
23 clearinghouse or validation center to ensure that
24 applications that are developed by communities or to ride
25 the whole network as a whole will not harm that network.

1 And so these are kind of some of the minimal
2 threshold requirements associated with what I call the
3 functionality of the network and clearly the
4 interoperability of the network to ensure that it remains
5 interoperable.
6 MS. GOMEZ: I've got a good one. Sorry. Don't
7 look at proprietary standards.
8 CHAIRMAN ROBINSON: I'm going to interrupt the
9 questions now because I understand that Robert LeGrande
10 is on the phone now. Is that correct? Robert, are you
11 on the line?
12 (Discussion held off the record.)
13 CHAIRMAN ROBINSON: No, Robert, we can't hear
14 you, but we are seeing that someone is hearing you
15 because your comments are being reflected on the screen.
16 Okay. We have to give them two seconds. Is there any
17 other question from a board member while we're waiting?
18 Brian?
19 MR. SHEPHERD: To kind of follow up on Diane's
20 point, and we've wrestled with this. You brought up the
21 physical versus the operational, and we've wrestled this
22 a lot I think throughout the deliberations. If you put
23 the minimum technical requirements at a physical level
24 and they meet a specific requirement, you can then
25 basically destroy that with faulty operational

1 implementation. How do you wrestle with that, so how do
2 you wrestle with ensuring that the technical requirements
3 we're coming up with are followed and implemented
4 properly at an operational level?
5 MS. GOMEZ: My response to that would be that
6 that is FirstNet's responsibility. I recommend that that
7 is an underlying concern, and it's an important concern.
8 But it is FirstNet's responsibility to make sure that it
9 operates the network according to the technical
10 requirements that it develops based on your input and
11 based on the RFPs and all the other activities it has to
12 undertake. So what you're doing as I said is you're
13 establishing the constitution. It's up to them to
14 operate according to that constitution.
15 MR. FONTES: I think too that just like in the
16 commercial world, anytime an antenna site is touched,
17 there is a checklist to make sure that there is
18 compliance with the operations of that sales site.
19 I think there also has to be some type of
20 mechanism to ensure that there is compliance with the
21 buildout functional aspects of that network, and whether
22 it's hiring third parties or if in fact there is a robust
23 market out there to ensure that the system is not
24 interfering or the system is working well that can
25 provide that information back into FirstNet. But there

1 will have to be initially an assessment as to whether or
2 not that network is being built according to the specs.
3 CHAIRMAN ROBINSON: Thank you. I think we're
4 still struggling with the audio back there. So are there
5 any other board member questions? If not -- oh, I'm
6 sorry, Steve. Steve, I've got to move through once and
7 then from the audience, and then we'll come back.
8 There is a question that we received via email
9 from Mr. Chris Spengaspar, and the question is would it
10 be appropriate if this public safety network started with
11 FirstNet managing and establishing at least two to four
12 nationwide LTE cores spread out across the United States.
13 The same thing with the commercial practice as opposed to
14 each waiver buying their own EPC core. So I'll open that
15 up to the board.
16 MS. GOMEZ: Well, I think I would just point to
17 the statute because the statute -- let me see if I can
18 find it. 6202 of the statute says that the nationwide
19 public safety broadband network shall be based on a
20 single national architecture that evolves with
21 technological advancement and initially consists of a
22 core network that's based on commercial standards and a
23 RAN that's based on commercial standards and developed,
24 constructed, managed, maintained and operated to take
25 into account the plans developed at the state,

1 local and tribal planning and implementation grant
2 program.
3 And the reason I'm just reading from the statute
4 is the statute clearly contemplates a core, not multiple
5 networks. Now it can be distributed and FirstNet can
6 make many decisions that the commercial carriers make
7 with regard to where their cores are placed, how many, if
8 there's redundancy concerns, those types of things. But
9 the statute clearly does not contemplate having multiple
10 networks that are tied together.
11 MR. FONTES: I think just the costs of that would
12 be rather prohibitive, and the idea is you're going to
13 have $7 billion to start this, and to start this for that
14 little amount of money is going to be extraordinarily
15 difficult. And that's why you're going to have to rely a
16 lot on commercially available technology,
17 MR. COHEN: That's the whole point of having a
18 single national governance body was to achieve the
19 economies of scale and bargaining power at the national
20 level that public safety hasn't been able to do on its
21 own to date. So I would just echo their comments.
22 CHAIRMAN ROBINSON: Thank you. Steve, you had
23 another question.
24 MR. PROCTOR: I was going to ask Bob to ask the
25 Board.

1 (Laughter.)

2 MR. PROCTOR: In your best visionary eye, where
3 do you see this process 60 months from today? Five
4 years.

5 MS. GOMEZ: Well, all right. So let's put
6 ourselves -- I'd love to ask Verizon that question
7 because they've had the development and the deployment,
8 and they're currently in their stages of deployment. So
9 five years from now, if I follow their model and I
10 understand their model, we have deployment in a
11 significant part of the country and we have service
12 that's being provided to public safety in a significant
13 part of the country.

14 Not only that, but we have significant rural
15 milestones, so it's going to be in parts of the country
16 that you're not necessarily thinking about but may be
17 from. So obviously we've seen the RFP process, we've
18 seen everything that's been developed from the RFP
19 process, and we will see significant deployment I think
20 in 60 months.

21 MR. FONTES: I think the 60-month marker and the
22 significant deployment that Anna is referring to will in
23 large part depend upon the cooperative and constructive
24 relationship between the commercial and public safety
25 sectors because there is going to be a lot of this riding

1 the commercial network just as there is today.
2 And I think that we have an opportunity to be
3 significantly down the road five years from now, just as
4 we have an opportunity if we're not working in a
5 constructive and cooperative way of creating our own
6 roadblocks if you will during that five-year path.
7 But I would certainly hope that the way this was
8 structured, with a single nationwide licensee, with the
9 Board, at least the representatives in the categories
10 that are on the Board, that there will be a great
11 opportunity to move this forward. This is a first-time
12 real opportunity for public safety to move into the 21st
13 century with interoperable broadband wireless services,
14 and it would be a horrible mistake to thwart that.
15 MR. COHEN: I share the optimism. I really hope
16 in five years there will be significant deployment. Part
17 of that reason is because the statute does direct
18 FirstNet to maximize the use of existing commercial and
19 other infrastructure, state and local and federal
20 government. And just with that alone is a great
21 headstart. So I too hope that within five years there
22 will be substantial use already in deployment, including
23 in rural areas.
24 CHAIRMAN ROBINSON: Well, I want to thank our
25 panelists this morning for participating. It's been very

1 informative for us, and I'm sure you can tell by the
2 questions that the Board is very engaged with your
3 remarks, and we'll be using them as we move forward in
4 our process. So thank you very much for participating
5 this morning.
6 We are now going to move directly into our second
7 panel. That panel will be moderated by Paul Steinberg,
8 and so I'm going to turn it over to Paul at this point,
9 and if the members of Paul's panel would come up.
10 MR. STEINBERG: All right. Well, that was pretty
11 smooth actually. I didn't know how that would work.
12 Good morning. First, I wanted to thank you gentlemen for
13 being here. We look forward eagerly to your remarks.
14 First, just briefly, now the rest of the workshop
15 will sort of parallel the three working groups that the
16 Board has established and is now working through the
17 process with. This is the first working group, and the
18 scope of this working group is around the topics of
19 standards, which we heard a lot about already, user
20 devices, test and conformance and evolution, which we've
21 also heard quite a bit about.
22 So we have a couple of you who are from the
23 vendor community, from Ericsson and Nokia Siemens
24 Networks, and I'll work my way through the formal
25 introductions in a second. We're hoping to hear from you

1 about how does this work in the commercial world, how do
2 you leverage standards, how do you achieve intervendor
3 operability and how do you work with your carrier
4 partners to do that.
5 The carrier representative looking for the
6 perspective from the other side as they procure
7 equipment, how do they achieve interoperability, how do
8 they evolve the network and how do they manage and make
9 sure that the interfaces are consumable over time.
10 And then finally, Tom, we're looking definitely
11 from the user community past experiences and your
12 perspective going forward about the importance and how
13 you see uniquely achieving interoperability around the
14 needs of public safety.
15 So, with that, I'd like to first introduce Tom
16 Sorley, who is the Deputy Director for Radio
17 Communications Services with the City of Houston and
18 Chair of the National Public Safety Telecommunications
19 Council, NPSTC, Technology Committee. Tom, we look
20 forward to your remarks. Thank you.
21 MR. SORLEY: Good morning. I think I need the
22 clicker. I think I should be able to figure this out.
23 It says next. I should be able to do that. First, thank
24 you for inviting us to present. I'm here representing
25 NPSTC, which is the National Public Safety

1 Telecommunications Council. We've been working on public
2 safety broadband issues since about 2006 and some of the
3 things that we've published and some of the work efforts
4 we've done to date.
5 In '07, we did a public safety broadband
6 statement of requirements to give you kind of a scale.
7 That was about a four-month effort and involved well over
8 500 vendor public safety industry partners in a
9 collaborative effort. That was published in anticipation
10 of the auction. We followed that up with a broadband
11 task force report that I believe both of these documents
12 have been submitted to the Board.
13 The broadband task force report actually focused
14 on the minimum requirements for interoperability. At
15 that time, we still did not have a defined technology and
16 we also didn't have a defined governance, so there was
17 significant effort in that report on those topics. Now
18 some of that's rather moot.
19 We recently published a local control document
20 that talks about what's meant by local control, what do
21 agencies really need to control, what applications, what
22 sort of things. And then we have a priority and quality
23 of service document that should be coming out next month,
24 and I believe we have submitted a draft of that document
25 to the Board.

1 So what are we doing coming up? We've begun a
2 process to update our statement of requirements. We have
3 roughly 200 active participants at the moment from
4 industry and public safety engaged in this effort. We
5 are planning to publish what we're terming a high level
6 version of that, which is similar in structure to the
7 original. We hope to have that done by August when we
8 have a defined work plan with writing groups assigned.
9 We plan to do a subsequent deeper dive of that
10 statement of requirements thereafter, and then I wanted
11 to talk a little bit about kind of what our process is.
12 We have a consensus process again with industry, with
13 public safety, trying to take the noise if you will of
14 the whole marketplace and bring it into more of something
15 that you can actually make sense out of. All of our
16 draft documents are vetted through a standardized process
17 through the industry, through the public safety community
18 and the general public if they so desire. And then
19 ultimately the final documents are approved by the
20 governing board before they're released.
21 And so what else are we going to be doing here?
22 We have some other work groups that I didn't put on
23 there. One, we have a very active security task group
24 work group that's ongoing, and I didn't mention that one,
25 mostly because the Chair of that group is on Panel No. 4,

1 so I'm sure he'll be mentioning that.

2 We also have a very big effort in mission

3 critical voice working group going on right now. We have

4 it broken up into two parts and we're doing a lot of work

5 on that. We hope to ultimately roll that into the SOR,

6 so that's why I don't have it listed as a work product on

7 the slide. That effort is like I say ongoing. We are

8 working on use cases for that right now, and it's looking

9 really good.

10 So what is NPSTC kind of recommending? Some of

11 the obvious things. Obviously the statute says long-term

12 evolution. We believe in the single PLMN ID. It's hard

13 to say, isn't it? We believe roughly in many of the

14 recommendations that are contained in the document that

15 the FCC I believe put on the record. We believe it's

16 important to prepare for IPv6 because IPv4 will run out

17 of addresses. So, if you're building a network from

18 scratch, you need to make sure it's future-proof.

19 Nationwide and local application administration,

20 it's important that you understand that some applications

21 will be nationwide while others will be local and

22 everything in between.

23 On the earlier panel, they talked about

24 applications in an app store. We believe that there will

25 be an app store as well, but we believe it's more towards

1 the Apple model with more strict controls than say the
2 Android model that is not. So there will have to be some
3 oversight.
4 We believe in a common nationwide prioritization
5 and QOS scheme. There will be a nationwide framework if
6 you will of priorities that we all agree on. That's the
7 way that it should be. There will be some let's call it
8 reprioritization at the local level that will be event-
9 based and role-based and those sorts of things. We still
10 believe in the preemption capability and most of that
11 having to do with emergency button activation and
12 critical life safety issues.
13 And then also we believe in the minimum cell edge
14 performance requirements because without throughput you
15 basically don't have a network. You have to have
16 operability to have interoperability.
17 And then generally speaking, we believe less is
18 more, especially as it relates to this group. Reaffirm
19 the LTE. Reaffirm the recommendations that the FCC has
20 already collected in the record. Clearly prohibit
21 proprietary technologies that could interfere with
22 interoperability, and lastly, we don't believe you ought
23 to make too many more conclusions than that as a Board.
24 FirstNet is charged with running this business, and if we
25 get too proscriptive, we'll end up tying their hands to

1 the fact that they won't be able to do their job.
2 And NPSTC is a consensus-based organization. We
3 broker information, and so I wanted to leave you with
4 this website. This is our new public safety broadband
5 directory. It's intended to provide information about
6 the partners that are involved in this work effort from
7 industry and from public safety, and I'd like to close by
8 thanking OEC and OIC for their continued support of NPSTC
9 and the work that we do.
10 We're all volunteers. We all have day jobs,
11 including our industry partners, and without their
12 continued support, we would not be able to get this work
13 accomplished. So we look forward to the questions.
14 MR. STEINBERG: Thank you very much, Tom. Okay.
15 Now we'll move to Ajit Kahaduwe, head of Industry
16 Environment, North America, Nokia Siemens Networks.
17 Ajit?
18 MR. KAHADUWE: Thank you. First off, I'd like to
19 thank the Commission, and the Interoperability Board for
20 inviting me and giving me an opportunity to present today
21 for Panel 2.
22 So, to get started, I want to address first the
23 3GPP baselines. There's four releases. Sorry for the
24 small text. For 3GPP, Release 8, 9, 10 and 11. Release
25 8 has been in operation already commercially. Release 9

1 we expect to see developed commercially in the next 12 to
2 18 months. Release 10 was finished a year ago. Release
3 11 will be finished by the end of this year based on
4 expectation.
5 The important thing here though is that when we
6 consider FirstNet and the time for it, Release 9 brings a
7 lot of interesting features that would be very valuable
8 for public safety and should probably be a good starting
9 point for the network based on current industry time
10 scales. But FirstNet should really consider as well that
11 it shouldn't be an early adopter of technology. We
12 should be following commercial deployments. That helps
13 to reduce risk, especially on these major system
14 releases, as well as improves stability and gives a cost
15 curve that's more beneficial to the network.
16 In addition, specific features which may come
17 from releases that are important to public safety, those
18 could be cherry-picked because we can't make hard and
19 fast rules because we know in the real world rules are
20 always broken due to expeditious needs.
21 Going on to the interfaces, in general, 3GPP
22 interfaces are interoperable. They've been getting more
23 interoperable from each release starting from GSM all the
24 way now to LTE. But the real definition, where we change
25 from academic standards to reality, is in the definition

1 of what's inside the specs and deciding that. In the
2 commercial world, we look at the standards, we have the
3 manufacturers and we have the operators and we work
4 together to identify the parts of the specs that we use.
5 This is important because blind compliance to the
6 standards isn't practical. What is developed is based on
7 market demand, not on the totality of every option.
8 So we recommend here that the basis are in the
9 specifications, but the functions and what is used on an
10 interface by FirstNet needs to be agreed with the vendor
11 community as well as the user community here. The other
12 thing we think as well is if we do some element grouping,
13 between like the MME and the eNodeB, we can further
14 optimize testing interface reductions.
15 Now, again going to the 3GPP release timeline, we
16 put out a new release every year, so you can see Release
17 9 was done two years ago, Release 10 was done a year ago.
18 So why not use Release 10 today? Well, it comes down to
19 this. Just because a specification is done doesn't mean
20 it's actually complete. It takes time to reach maturity
21 in the spec, so for public safety especially, it isn't
22 valuable to run out and get the latest spec. You should
23 look forward to what's in the new specs, but to ask that
24 as a requirement on the beginning software side is
25 dangerous because it takes time for the vendor community

1 to go through and verify what's in the specs and to
2 develop. So we see over a two-year period a great
3 reduction in the number of change requests in 3GPP.
4 Looking at the subsystem idea, we encourage and
5 need open competition and interoperability, but that
6 comes in the face of testing. So it's very important as
7 well that we are able to look at the subsystems and group
8 elements together so that we can reduce the testing
9 complexity for the network. Otherwise, you get into
10 basically becoming a large test house versus deploying a
11 network.
12 Going on, let's look now further at the standards
13 bodies. There's quite a few standards bodies that could
14 be referenced. In general, the main ones -- and this may
15 not be limited obviously -- are 3GPP because that's
16 building the network. That's the transport layer for
17 every packet in the network with certain applications
18 like SMS, voice over LTE.
19 OMA is a very good place as well for looking at
20 multimedia messaging service, device management specs
21 that could be enhanced for public safety. IETF, without
22 saying, is important because it's the protocol house that
23 we have to choose from for many packet-based
24 implementations and the IPv6 before spec especially
25 there.

1 ATIS has a place as well in this, as does TIA.
2 ATIS does the commercial mobile alert service, PLM
3 numbering, PSAP interworking. GSMA is important because
4 that's the operator and vendor community on how to
5 interwork, so there we have profiles for voice over LTE,
6 the RCS profile for rich communication suites, roaming
7 guidelines, and then TIA with ATIS can work on P25
8 interworking.
9 Regarding new and novel features that are going
10 to be developed, we know they're going to happen, but
11 it's really important that those are brought to a
12 standards body. We need to have openness, and they need
13 to be developed within a standards construct so every
14 manufacturer has an opportunity to develop a feature.
15 On evolution, 3GPP releases are backwards
16 compatible, but in the real world, we need to look at how
17 it's really done, where we first test in a vendor
18 environment, then in an operator test lab and finally to
19 a first office application. Before we roll out to the
20 network, it is common that we have software releases and
21 system releases, but we need to look forward in the
22 roadmaps of the vendors with FirstNet and say, you know,
23 another year, these are my requirements, because we need
24 to synchronize the feature availability. Just to come
25 within a month and ask for a feature is not reasonable

1 and you won't have availability across a national
2 network.
3 So it's very important to coordinate the
4 stakeholders and also to follow commercial deployments.
5 Again, I can't reiterate that because we want to minimize
6 the testing learning curve and the costs.
7 FirstNet itself has three choices. Either
8 develop its own testing capability, have a qualified
9 third party for outsourcing or to work with vendors to
10 develop the testing capability on the fly.
11 The testing world is an ecosystem with a
12 multistakeholder environment. PTCRB in the North America
13 market and GCF internationally does conformance for
14 network elements. We actually do interoperability
15 testing, and that's done in the network world with NVIOT
16 for the equipment manufacturers and MSF and operator test
17 beds for the practical part.
18 And this is just giving an example of how we can
19 do testing starting from specs to conformance to IODT
20 requirements. It is a multistakeholder environment.
21 Testing everything to the letter is not the end of the
22 game. It's testing what you need, and that's what's
23 important here in testing.
24 And finally I'll leave you with some small
25 remarks on IPv4, v6. We need to start with the dual

1 stack so that when we're ready for v6, we're ready to
2 implement in the network. Don't constrain yourself to
3 v4, GTP on S5, and look at a second PLMN ID for secondary
4 users like utilities. That gives you more flexibility in
5 IDs and numbers on top of the common single PLMN ID for
6 public safety. Thank you.
7 MR. STEINBERG: Thank you, Ajit. Okay. Now
8 we'll move to Patrik Ringqvist, Vice President, Wireless
9 Network Solutions at Ericsson. Patrik.
10 MR. RINGQVIST: Thank you, Paul, and thank you
11 for giving me the opportunity to be here this morning to
12 address you. So let me start out. My scope for today,
13 I'm going to talk a little bit about multivendor
14 interworking. And as you have heard from Ajit, standards
15 is the foundation for interoperability. We do a lot of
16 work in standards to ensure that they are robust and
17 enables multivendor operability, but it is not enough.
18 There are a number of things that are done in the
19 standards that perhaps are not conducive to
20 interoperability. It is a consensus forum. There are a
21 number of things put in the standards and many, many
22 options, and there is room for interpretation.
23 So standards are important, but they are no
24 guarantee for interoperability. I think you all need to
25 recognize that. But it's not doom and gloom, right?

1 Every operator that I know of is a multivendor network
2 environment and it works. Interoperability works.
3 So obviously the industry has learned how to live
4 in this environment and how to pick the right things out
5 of the standards and how to work together to make the
6 various elements be interoperable.
7 There are also a large number of interfaces being
8 defined in 3GPP. So I think it is very important that
9 you look at those and employ strategies that you minimize
10 the need for interoperability testing.
11 Ajit talked about grouping, and I certainly agree
12 with his views there, that a grouping and a deployment
13 strategy that limit the need for interoperability testing
14 needs to be adopted. At the same time, it's also very
15 important to align with how the commercial world is doing
16 interoperability testing to secure interoperability not
17 just within the national public safety network but also
18 with the commercial networks for roaming purposes and
19 other things like that. So do align with the commercial
20 world.
21 I'm going to take you through one example of how
22 we at Ericsson approach interoperability, and I'm going
23 to focus on the interface that's probably the most
24 important interoperability interface, the air interface,
25 the interface between the user equipment and the networks.

1 So, in this slide here, you see four activities
2 that we are using at Ericsson to secure interoperability,
3 and I want to point out that we go through all these four
4 activities before an operator sees the device. This is
5 done by the vendors prior to releasing terminals devices
6 to the operator for their part, and I'll come back to
7 what they are doing.
8 So, first and foremost, it starts already at
9 standardization time when network vendors like Ericsson
10 and terminal vendors collaborate on standards to ensure
11 that the standards do have the right feature set to
12 enable interoperability.
13 The second piece is the implementation is done to
14 meet the market needs. So there are a number of optional
15 features and there are a number of optional services.
16 There's roadmap discussions aligning development so that
17 we align development in terminals and network is very
18 important. And at Ericsson, we have roadmap discussions
19 with all the major chip set vendors and terminal vendors.
20 This is an important piece to ensure that the features
21 arrive at the same time and that we have the same
22 interpretation.
23 The next piece is development testing. Here we
24 do testing during the actual R&D phase before the
25 software is ready to early on catch fault issues, so this

1 we do together with the leading chip set manufacturers
2 and terminal vendors.
3 And the last piece is what we call multivendor
4 terminal verification, and this is where we in our labs
5 test devices against our infrastructure to ensure that it
6 is interoperable. And again all of these activities are
7 done prior to the operator actually seeing the devices.
8 So IODT, I talked a little bit about this, so
9 this is primarily then in the R&D phase before the
10 software and the devices are ready, and it's primarily
11 focused on 3GPP validating our interpretation of 3GPP
12 standards, that we are aligned, that it works together.
13 The multivendor terminal verification, we do that
14 using equipment in our labs, and then the operators can
15 bring in their equipment and their devices or the vendors
16 can bring in their devices and work together.
17 So this is an activity that we do with many
18 terminal vendors, and we do it in a global setting so
19 they can work on all the networks around the globe.
20 So if you put it all together, I talked about the
21 steps that happens before the operator sees it. In here,
22 you have these red, yellow, green stoplights, so to the
23 left of that, that's where the vendors do their work and
24 to the right is where the operators do their work. And
25 it's important to note that the vendors do a lot of

1 activities before releasing to operator environment to
2 ensure interoperability, and this is to ensure for a
3 number of reasons.
4 It is to ensure that the operator activity goes
5 smoothly, but it is also to reduce costs because we don't
6 want to repeat all this interoperability testing for
7 every operator. So the vendors do it once and then we
8 release it to the operator to do the operator-specific
9 things.
10 So here I talked about what's valid for a
11 terminal, but similar principles are applied also for the
12 network element and network element testing. The same
13 type of process is done for standardization. We align
14 the feature set, we align and do testing in our lab
15 environment through industry for us before we release it
16 to an operator environment.
17 The operator typically does two things:
18 acceptance testing and field testing or FO activity, and
19 in some cases this acceptance testing is very limited.
20 It's just to make sure that the baseline quality is good
21 enough, and the real focus is on the FO activities or the
22 field testing. But this is something that differs a
23 little bit from operator to operator and is dependent
24 upon the operator's environment and their situation.
25 So I want to leave you with some final words,

1 that of course multivendor testing is needed, but it's
2 not a strange thing. It happens every day, and we work
3 with all the major manufacturers, both infrastructure and
4 device vendors, to ensure interoperability is working
5 before it's released to the operator. It's important to
6 understand this clear division of responsibilities
7 between the vendors and the operators so that when we do
8 develop a testing interoperability strategy, we do a
9 minimum of replicational tests to ensure maximum usage,
10 and that's the whole purpose here and at the same time
11 ensure that we have a right balance between the costs --
12 the costs of doing a lot of interoperability testing can
13 cost a lot. Time to market, it can take a long time.
14 But of course we need to eliminate risks, so that
15 right balance there, and that may differ from an operator
16 to operator environment. Thank you very much.
17 MR. STEINBERG: Thank you very much, Patrik.
18 Okay. Our last panelist is Martin Dolly, Lead Member of
19 the Technical Staff, Core Network and Government
20 Regulatory Standards for AT&T. Martin.
21 MR. DOLLY: Good morning. I appreciate the
22 opportunity for speaking here. If I'm a little tired, I
23 just got back from a 3GPP CT 134 meeting in Taiwan on
24 Saturday and then took the train down here.
25 MR. STEINBERG: Is Release 11 done now?

1 MR. DOLLY: For CT Release 11, it will be done in
2 September.
3 MR. STEINBERG: Okay.
4 MR. DOLLY: And actually at the meeting, I had a
5 CR on 911, location by value being passed from the
6 location function down to the EECSEF, okay? All right.
7 Okay. Standards are important in that they
8 provide a key framework for interoperable products.
9 Without standards it would be difficult, if not
10 impossible, to have interoperability. But standards by
11 themselves do not ensure interoperability, and the way to
12 think about it is that standards get you to the ballpark,
13 right? But it doesn't get you to your seat. And so you
14 achieve maybe 85 percent of interoperability with
15 standards, but you need to do conformance testing in
16 order to, like I said, get you to your seat and actually
17 achieve interoperability.
18 Within the standards, whether it's LTE, a ball
19 packet core, there is a lot of options, and in addition
20 to the options, you have variations from vendors, okay?
21 Some of that's due to IPR. In addition, carriers like
22 AT&T, we want to provide enhanced services and
23 differentiate ourselves, and so there is differentiation
24 in the products as well. Ultimately it's through carrier
25 requirements and industry implementation guidelines that

1 define the set of standards to support interoperability
2 across networks.
3 As a carrier, intervendor interoperability, we
4 base our product requirements on standards and specify
5 these to the vendors, and we test, test, test. The
6 bottom line is we use industry forums as well as within
7 our labs to test and verify. And when it comes to
8 testing, we also do regression testing to make sure that
9 capabilities we have deployed in the network don't break
10 as an example, and I know I'm going to run over on time.
11 Given standards are full of options. There are
12 cases where vendors may interpret the standards
13 differently, and actually to that end, though we're
14 working on Release 11 in 3GPP, as we are deploying LTE in
15 our networks, AT&T and other carriers, we're finding
16 there's bugs and there's holes.
17 And so as part of the standards process, we go
18 back and make corrections, and so what you're going to
19 see within the 3GPP standards, you know, starting now
20 because we're getting real-life experiences, we are
21 bringing in those corrections to the specifications, and
22 it takes time for those corrections to be made.
23 Okay. Standards conformance. Okay. So, within
24 3GPP, there's the RAN 5 Group where they actually develop
25 the conformance testing specifications, and basically

1 it's between the UE and the network. There's actually
2 further refinement. As Ajit mentioned, within GSMA, IR92
3 defines interoperability between the UE and the network
4 to help facilitate roaming between operators. Initial
5 LTE deployments are typically going to be within a whole
6 network, and sometime I guess around 2013 or '14 we'll
7 see roaming between carriers. IR94 defines the standard
8 for video interoperability between carriers.
9 As mentioned in Ajit's presentation, the PTCRB is
10 a North American organization that defines the standard
11 for independent evaluation and certification of wireless
12 products, starting with GSM, UMTS and moving forward with
13 LTE.
14 With respect to public safety, the standards
15 forms that are applicable are of course RAN 5, ATIS. I'm
16 Chair of the PTSC Packet Committee within ATIS, and in
17 addition, the WTSC where they do the CMAS standardization
18 as well and the PTCRB for testing.
19 And I'm running late. I'm going to jump to the
20 end. Okay. So standards do not ensure interoperability
21 in and of themselves. I mean, they get you in the
22 ballpark, but you need to do certification testing in
23 order to ensure product interoperability. Proprietary
24 implementation of standards can lead to lack of
25 interoperability. Conformance testing is important to

1 ensure a minimum level of performance, and testing
2 doesn't stop there. I mean, we constantly do testing,
3 and we do retrotesting, as I stated, to make sure that
4 whatever we deployed isn't broken. And the evolution of
5 standards must ensure backwards compatibility while
6 introducing new capabilities. That's it.
7 MR. STEINBERG: Super. Thank you very much,
8 Martin. Gentlemen, thank you very much. I think now I
9 would turn to my fellow Board Members and see if there
10 are any questions. Dereck?
11 MR. ORR: I have one, Paul.
12 MR. STEINBERG: Go ahead, Dereck.
13 MR. ORR: I have several, but I'll start with
14 one.
15 MR. STEINBERG: Well, you get one.
16 MR. ORR: I would love for the panelists,
17 especially Ajit and Patrik and also to get Martin's take
18 on this. You spoke about groupings of subcomponents and
19 subelements, but you didn't get very specific on what you
20 meant by that. Can you go into a little bit more detail
21 about what you're referencing when you're talking about
22 groupings to minimize testing requirements? And then
23 after both of you do that, if you could comment on that,
24 that would be very great, Martin. Thank you.
25 MR. KAHADUWE: Okay. So, in reference to the

1 groupings in my slides, I gave an example, but it's an
2 idea of taking subsystems like the MME and eNodeB
3 together, S-Gateway, P-Gateway together. You can even
4 throw in the PCRF if you want.
5 We still need open interfaces and compliance to
6 what FirstNet wants, but in terms of reducing the
7 complexity where we don't have every element testing with
8 every other element for interoperability where you get
9 this permutation that goes kind of into an expediential
10 mode, by putting element blocks together as kind of
11 legos, then we can reduce the actual interface testing.
12 MR. ORR: Can I ask a clarification question?
13 MR. KAHADUWE: Sure.
14 MR. ORR: When you say putting them together, are
15 we meaning in a single vendor solution?
16 MR. KAHADUWE: Right. Sorry.
17 MR. ORR: Okay.
18 MR. KAHADUWE: Yes, specifically in a single
19 vendor solution. That will help. Like I said, we still
20 have to make sure that everyone does conform to the
21 interfaces, but for interoperability testing and ensuring
22 that that happens in an optimal way where we don't spend
23 the next two or three years testing every interface times
24 every vendor, the only practical way even in the real
25 world is we group subsystems together within a vendor

1 ecosystem.

2 MR. RINGQVIST: So I agree with Ajit's comments

3 there, and I would also like to add that grouping does

4 not necessarily preclude that you have a multivendor

5 network. There is also the concept of regional

6 deployment where you may in a region be grouping certain

7 vendors and in another region you may have a different

8 vendor.

9 What you can see though is when you're going into

10 industry that there are a number of interfaces that are

11 probably the most commonly from interoperability and

12 others that are less, so you look at that and make a

13 choice, a person can make a choice on that. And they did

14 and it's still early, so there is still I think a lot of

15 activities and a lot of work that needs to be done to

16 mature some of these interfaces from a vendor

17 interoperability point of view.

18 MR. DOLLY: Okay. So speaking as a carrier, we

19 need multivendor, and we need to have them interoperate

20 within our network. With respect to grouping, some of

21 the lessons learned with the iPhone and the volume of

22 data traffic within our network, we are relooking at the

23 grouping of the elements and how the elements are

24 deployed within the EPC in order to get greater

25 efficiencies to handle the data traffic.

1 MR. STEINBERG: Questions from the Board?
2 MS. DECKER: I heard you talk a lot about the
3 importance of public safety not being an early adopter of
4 technology. We deal with that I think a lot, and I agree
5 with that concept. But given the charge of the Board to
6 set technical specifications, I'm struggling with how we
7 would put that into a technical specification. That
8 seems more operational to me, and yet I think it's a very
9 important point that we want to get there.
10 So I'm looking for advice from the panel as to
11 how we would say or how we would move our
12 recommendations, our technical recommendation, to say at
13 what point does this standard become something that we
14 really should think about moving forward with?
15 MR. KAHADUWE: So, yes, that's actually a very
16 good question because to know when the cake is baked is
17 kind of a problem because we don't have a skewer to stick
18 into it.
19 Looking at commercial operation is one
20 methodology of understanding where a standard is. We
21 know today, for example, Release 8 is widely deployed,
22 that's what's there. I think you need to look at
23 starting points for the network, kind of projecting a
24 little bit ahead, and make a few assumptions about where
25 standards may be. But you don't set the end goal, right?

1 You'd be a little bit conservative in your approach.
2 Also look kind of around the industry a bit about what is
3 actually showing up in products or what's expected in the
4 implementation in the next 12 months as a starting point
5 to the network.
6 And I'm sure Martin from AT&T can give some
7 comments as well about the practicality, but generally I
8 think when you have a standard, you can look at it and
9 within 12 months you kind of have some stability, and at
10 24 months, you have very good stability. Then the real
11 question is, is going to use it, right? And that's
12 another issue you have to look at. Just because a paper
13 is written doesn't mean it's going to be implemented by
14 vendors, because market demand has something to do with
15 that.
16 MR. DOLLY: Yes. I mean, I also support our GETS
17 program and WPS program within AT&T, and so our advice to
18 the NTS program folks is to ride our deployment curve and
19 that you can get greater efficiencies with costs and
20 deployment if you are incremental on what we are already
21 deploying and doing.
22 MR. STEINBERG: Other questions from the Board?
23 Tom.
24 MR. SORLEY: Mine is kind of a nontechnical
25 answer. I think one of the keys for FirstNet moving

1 forward and not necessarily the interoperability board is
2 to become a player with the other vendors, and road-
3 mapping, I think you heard Patrik mention road-mapping at
4 least twice in his presentation. And I think it's a
5 critical element moving forward is that there is some
6 active road-mapping. You know, public safety typically
7 is just a customer, and with FirstNet, we now have a seat
8 at the table. Obviously it's a business table, so we
9 understand that.
10 But getting into the standards development and
11 getting your needs out there from a road-mapping
12 perspective is probably the most critical. I don't think
13 that really helps you bake your cake, but I think from a
14 strategic perspective, we're going to be in a much better
15 place hopefully moving forward than we are now.
16 MR. STEINBERG: Steve, before I go to you, could
17 I follow up real quick, Tom. On the topic of road-
18 mapping, as a user of technology, do you have a sense for
19 what horizon roadmap needs to be out there for you to
20 contemplate? Is it two years, five years, 10 years?
21 MR. SORLEY: So I have a very good sense in a LAN
22 mobile world. The problem is I don't have a very good
23 sense in the data world. It changes so rapidly that a
24 lot of it as they said is market-driven. I have a
25 fireman that likes to tell me, tell me where the next

1 fire is and I'll tell you where I need coverage. It's
2 kind of the same concept is what's the next latest thing,
3 and so I think in many instances we're a bit ignorant of
4 the market and how it operates, so it's difficult to do
5 that. But in general we are very slow adopters, so our
6 budget cycles are long. If we adopt things quicker than
7 five years, in five-year cycles, it's a miracle, and as
8 technology resets every what, 24 months, 36 months.
9 MR. STEINBERG: Twenty minutes.
10 MR. SORLEY: Twenty minutes, we're never going to
11 be there. We're going to constantly be catching.
12 MR. STEINBERG: Okay. Thanks, Tom. Steve.
13 MR. PROCTOR: First of all, I just wanted to give
14 a shout out to NPSTC, Tom. You and your group and all
15 the supporting groups that have provided work with
16 respect to the list of documents you have, they've been
17 very helpful, and we're gratefully appreciative of that
18 work.
19 My question to all of you is this. What place or
20 what part do you see mission critical voice being with
21 all this network development? Do you see this eventually
22 being the mission critical voice system as well as the
23 data system long-term?
24 MR. RINGQVIST: I can try to give that a shot.
25 The mission critical voice is of course something that is

1 I'll say difficult to answer because it means different
2 things to different people. So again you referred to
3 NPSTC. NPSTC did a definition of what mission critical
4 voice is, and I think based on that definition, at least
5 in this phase, does not support mission critical voice.
6 This is one of those roadmap items. A discussion
7 needs to happen, a roadmap needs to happen in standards
8 and with the industry to plan it out in time when it is
9 feasible, whether it should be moved from the LMR
10 networks, existing LMR networks, to an LTE broadband
11 network, I think that is something that the user
12 community has to decide together based on that reality
13 that they are in and the needs that they have for
14 broadband access vendors.
15 MR. DOLLY: Okay. So again going back, it's sort
16 of analogous in support of government emergency services
17 and WPS. We have been working with NCS in bringing in to
18 3GPP the ability to provide priority for the signaling
19 and the handling of the media for both voice and data for
20 mission critical services.
21 MR. KAHADUWE: So, from my perspective, PSCR as
22 part of NIST has been a very good focal point for getting
23 the requirements for mission critical voice and direct
24 mode of operation and to bring that to 3GPP.
25 As Martin said, we have a way of handling already

1 the federal requirements for telephony type services as
2 well as data services, so there is a path to bring it
3 there to 3GPP and to other standards bodies.
4 So the end goal should be for mission critical
5 voice to be on LTE. Certainly it's not where we are
6 starting from, but over the time scale of this network
7 rollout, it definitely has to be part of the network
8 because the network should be serving all the needs of
9 public safety as a data network.
10 MR. SORLEY: I obviously have some comments on
11 that. I think there's no doubt that LMR is going to be
12 here for a while because we don't even have a standard
13 yet that really accomplishes the requirements of mission
14 critical voice. We're working on flushing out some more
15 in-depth detail on what is behind kind of the definition
16 that Patrik talked about, what are the key elements, what
17 are the things we have to have.
18 And we need to capture that, publish a document
19 and make sure we feed it into the standards process. But
20 as a local government employee, I can tell you that we
21 are in the final stages of completing the largest IT
22 project in the history of the City of Houston, LAN mobile
23 radio. We cannot continue to long-term over, you know,
24 years support multiple networks to achieve
25 communications. It's too expensive. And so we need the

1 new network to support mission critical voice, but it has
2 to be able to support the model, the requirements of
3 achieving, because our motto is first time every time,
4 and when you push the button, it's got to go through the
5 first time every time. And you've got to have devices
6 that you can carry into a fire, you have to have certain
7 things, and they're nonstarters, and if you don't have
8 those, it doesn't matter how good the business case is,
9 you can't do it.
10 And so we strongly believe that this new network
11 needs to eventually be able to do mission critical voice.
12 Will it be quick? Probably not because we have a lot of
13 nonstarters. We have to get there.
14 MR. STEINBERG: That's great. Thanks, Tom. I
15 think with that, I think we're going to have to close at
16 the top of the hour, so let me just thank Martin, Ajit,
17 Patrik and Tom for your remarks and diligent responses to
18 our questions. I believe we have a 15-minute break now,
19 and we'll reconvene with the next panel at 11:15. Thank
20 you very much.
21 (Whereupon, a brief recess was taken.)
22 VICE CHAIRMAN BUDKA: Good morning, and welcome
23 to our third panel discussion of the morning. This panel
24 discussion focuses on some of the key elements of the
25 public safety broadband network that touch some of the

1 aspects that make public safety communications public
2 safety communications: greater service, priority of
3 service, quality of service and also mobility and
4 handover.
5 We are joined today by four distinguished
6 panelists who will be addressing these issues from a
7 variety of different perspectives. We're joined with Pat
8 Amodio, Chief Engineer, of the DHS Joint Wireless Systems
9 Program Management Office, U.S. Customs & Border
10 Protection; Roger Quayle, Chief Technology Officer and
11 Co-Founder of IPWireless and hopefully speaking to us
12 from the State of Wyoming will be Robert Wilson,
13 Telecommunications Manager, Wyoming Department of
14 Transportation, State of Wyoming.
15 And speaking to us from Arizona, Scott Somers,
16 who is Vice Mayor of the Mesa City Council in the City of
17 Mesa, Arizona. Mr. Somers also serves as a hazardous
18 materials specialist and EMS Captain in Phoenix,
19 Arizona's Fire Department.
20 So, without further ado, I'd like to please turn
21 it over to Pat Amodio. Thank you, Pat.
22 MR. AMODIO: Thanks, Ken. First, I want to take
23 the opportunity to thank the board for selecting DHS and
24 myself to speak today and offer some insight into the
25 minimum technical requirements and possibly some future

1 design and RFP requirements.

2 Okay. A little bit of background quick. DHS
3 operates and maintains one of the largest technical
4 communications networks. These networks are currently
5 undergoing updates to meet federal mandates, better
6 security and improved capabilities. In fact, our users
7 have requested the need for data and video in addition to
8 mission critical voice and building, owning and operating
9 stovepipe type systems or otherwise a HDHS component that
10 owns and operates their own networks as inefficient and
11 not sustainable.

12 Our vision from a mission perspective is we need
13 voice and advance communications to do our jobs. We're
14 looking for solutions that provide situational awareness,
15 location-based services for efficiency and safety of our
16 agents and officers, data for developing common operating
17 pictures to more efficiently utilize our resources and
18 voice and data communications to improve coordination and
19 communications with our interoperability partners.

20 So the new DHS approach. DHS would like to
21 migrate from the own and operate model to a subscription-
22 based model approach, leveraging commercial broadband and
23 the national public safety broadband network. An added
24 benefit of this approach is that it provides a migration
25 path from current P25 voice only systems to broadband.

1 We want to leverage commercial technologies and standards
2 which will provide economies of scale by sharing costs
3 over a large user community and reducing lifestyle costs.
4 However, we need a mission critical grade of
5 service on commercial technologies to ensure that
6 communications are reliable and secure. So federal first
7 responders' hope is to be a customer on this network, but
8 realize there are many discussions that will need to take
9 place before this happens.
10 Here are some examples of scenarios that our
11 users have put together which address technical broadband
12 services. For instance, officers doing a background
13 check in a jetway and would like to determine if a
14 passenger has filed proper documentation. Another
15 example might be biometric identification checks, for
16 instance, fingerprinting and face recognition.
17 Now I'll discuss some of the topic areas for the
18 Board's consideration relevant to the development of the
19 minimum technical requirements and future RFP and design
20 guidelines.
21 So organizations have various geographical and
22 economic constraints and require deployment flexibility
23 for their broadband networks. We feel that data rates
24 can be based on minimum user requirements for various
25 applications. It's critical that they're based on the

1 applications. So, for instance, as an example, short
2 video or still frames can be transmitted if that meets
3 the mission or the minimum requirements. That's how the
4 data rates should be specified, not on full motion video
5 but basically on the minimum requirements.
6 Especially in rural and U.S. border locations,
7 these constraints necessitate the radio design provide
8 adequate coverage first and foremost and then capacity
9 for the broadband networks. So again at the bottom, it's
10 just an example of meeting the mission requirements with
11 the minimum application desires.
12 So capacity needs are dynamic, and we feel that
13 right-sizing the backhaul is also a concern for both
14 urban and rural areas. As an example, we feel that the
15 Board should consider some minimum backhaul requirements.
16 The concern might be that if there's no minimum
17 requirements set, then, for example, in a rural area, if
18 someone were to have let's say just six T-1s at a site or
19 roughly 10 megabytes of backhaul, if there's any kind of
20 surge with say three or a dozen users come into the area
21 and there's ideal radio conditions, they could consume a
22 lot of band width and interoperability may not be met
23 because there's not enough backhaul requirements to meet
24 the demand of the users.
25 Also, it's questionable that 4G companies will

1 cover the least dense portion of the U.S., so designs
2 need to take into consideration all commercial, federal
3 and utility sites, basically take into consideration all
4 assets that are available when considering the design of
5 the network.
6 Sullage data rates are a function of basically a
7 signal to interference and noise ratio and also intersite
8 distance, site antenna heights, radio frequency
9 environment and interference. So we feel that the data
10 rates should be based on the minimum user requirements
11 and the various applications. As I said previously,
12 probably not one size fits all, but they should be based
13 on the applications.
14 The last point, tower space, is constricted
15 because companies are already deploying 4G. Basically we
16 feel that maybe a future requirement for either design or
17 RFP, but time, money and productivity can be saved in the
18 RF design phases by utilizing mechanisms that are out
19 there to consider only locations that are available to
20 deploy equipment. So taking into consideration maybe
21 databases or the nationwide tower companies may have
22 databases that already consider towers that are fully
23 loaded and just rule them out and not consider them in
24 the design process. That's it. Thank you.
25 VICE CHAIRMAN BUDKA: Great. Thank you very

1 much, Pat. We're going to reach to the phone. Scott
2 Somers? Scott, are you on the line?
3 MR. SOMERS: I am.
4 VICE CHAIRMAN BUDKA: Oh, the miracle of
5 interoperable communications demonstrated here. Thank
6 you, Scott. We'll go to Scott, and then we'll go to you,
7 Roger. Thank you. Welcome, Scott.
8 MR. SOMERS: Thank you. Well, I don't know how
9 interoperable the communications are. I was going to try
10 to be on video, but apparently PCs and Macs don't work
11 together, so so much for that.
12 I do have some of the video, so I can watch as
13 the line goes through, and I'll be able to ask you just
14 to change the slides. Kenneth asked me to participate
15 today more along the lines of what the Fire Service
16 envisions the uses of this system will be both in the
17 short-term and the long-term, but we wanted to touch a
18 little bit on the interoperability, the history of our
19 systems and what we have now and where we're going.
20 From the perspective of interoperability, it
21 seems that the Fire Service has had challenges with
22 interoperability for a long time, and it's not just
23 communications. I know there is a D.C. Firefighter on
24 the Board, so he'll appreciate the analogy of our hose
25 couplings not working together. A hundred years ago, if

1 you tried to hook one hose from one city to a fire truck
2 from another city, you were just not able to do that.
3 You would think over the past 10 decades we would
4 have resolved that issue. Unfortunately, even here in
5 the valley and the Phoenix metro area, Phoenix has
6 different hose couplings than Chandler or even Mesa.
7 That's difficult enough, but -- are you still hearing me?
8 VICE CHAIRMAN BUDKA: Yes, we are.
9 MR. SOMERS: Oh, great. But when you can't talk
10 to one another, that makes emergencies even more
11 difficult, and so communications has improved over the
12 past decade but still faces some pretty significant
13 challenges and one of those is while voice communication
14 is absolutely essential to our fire ground operations,
15 really communication is becoming more and more about
16 data. The systems we have right now just are not able to
17 transfer that data.
18 In the past, public safety agencies typically
19 operated in communication silos, and so what happened
20 after particularly 9/11 and the safety challenges it
21 presents, each jurisdiction, even each department, used
22 different technologies and devices from different venues.
23 Thus, neighboring public safety agencies couldn't
24 communicate with one another on their radios and on their
25 networks. The answer to that has been that many

1 jurisdictions have added radio gateways that can
2 interoperate multiple radio frequencies, but that's
3 surely not a long-term solution.
4 LTE has the advantage of standardizing protocols
5 and interfaces so that more public safety personnel can
6 talk to one another, and what's extremely important about
7 these systems is that there are roaming capabilities that
8 are built in. This is particularly important for task
9 forces that are often created quickly and can bring
10 together individuals from numerous agencies who may not
11 have worked together before.
12 LTE eases the burden of providing strong
13 communications among newly assemble groups to provide
14 secure interoperability. The broadband data network can
15 make it easy to collaborate not just with voice but video
16 and multimedia data as well.
17 The next slide talks about LTE priority access,
18 and if there was one thing to take away from the
19 presentation here as something that the fire department
20 and the emergency services is we need to have
21 prioritization so that the mission critical data that we
22 need to get across the network gets through. The problem
23 with communications as it exists today is that it is
24 susceptible to congestion. What we're dealing with right
25 now is the situation where some agencies are deploying

1 WiFi hot spots, and those WiFi hot spots have very
2 limited range. Coverage isn't very good, so it generally
3 doesn't work well for us in the public safety
4 environment.
5 Some agencies have broadband through commercial
6 providers, and this allows them to have access to web and
7 email and some data transfer. But again those networks
8 get congested during emergencies and large-scale events
9 just when public safety communication is becoming most
10 critical. I mean, part of the problem has been that
11 these systems are built on 3G networks, and 3G networks
12 work fine when my children are trying to surf the web.
13 But it doesn't really give public safety what it
14 needs. 3G has inherited some limitations from the
15 network architecture used in 2G cellular systems. 3G
16 isn't nearly fast enough for public safety where really
17 seconds and minutes can count. It's limited to the five
18 megahertz bandwidth, so it doesn't have the flexibility
19 and range of deployment options that LTE has. It can't
20 properly handle high speed applications when numerous
21 users are on the system. It doesn't have the available
22 spectrum and efficiency of LTE. The latency is too high
23 for demanding real-time services, such as video, and the
24 real-time data that we are focused on.
25 VICE CHAIRMAN BUDKA: Scott, sorry to interrupt,

1 but I just want to make sure --

2 MR. SOMERS: The network architecture is complex,
3 which adds to our overall costs, and there is a city
4 council member who is dealing with the Topaz radio system
5 and very sensitive to the costs of these systems, and
6 it's really not optimized for IP, which is unfortunate
7 because IP is becoming increasingly common.

8 VICE CHAIRMAN BUDKA: Scott, sorry. I just
9 wanted to give you a time check. You have a little bit
10 less than a minute. Thank you.

11 MR. SOMERS: Okay. A little less than a minute.
12 So what I would like to do is skip down to a couple of
13 slides and just identify some of our current needs and
14 future needs because this was part of the conversation
15 that was held earlier about what are the minimum
16 standards and what do we need now.

17 And since LTE is evolutionary as in its name,
18 what the current needs of the system are gives you some
19 ideas of the direction we need to head immediately. We
20 have ADL systems, computer-aided dispatch systems,
21 sending and receiving documents and the ability to
22 transfer. I like what the previous speaker said about
23 short video because the ability of teams to send short
24 video back for real-time information to our command
25 center is extremely important for them to make decisions.

1 Over time, we would like to see that transmission
2 of incident video expanded so that we can have more real-
3 time data. We're looking at wellness and safety
4 monitoring in real time of our firefighters and police
5 officers so there is mobile accountability systems,
6 particularly in hazardous incidents, and electronic
7 incident command tracking to connect records management
8 systems and maintain our instant command worksheet.
9 So, with these last four slides, you can see how
10 what we hope in the fire service is an evolution of this
11 system for meeting our demands today in communications,
12 voice communications and some limited data and
13 transitioning that over time.
14 VICE CHAIRMAN BUDKA: Thank you very much, Scott.
15 I'll now turn it over to Robert Wilson. Is he on
16 the phone? Robert, are you there?
17 MR. WILSON: Yes, I'm here. Can you hear me?
18 VICE CHAIRMAN BUDKA: I can. I think maybe we
19 will move just straight to Robert, please.
20 MR. WILSON: I'm going to try this video bridge.
21 Hang on just a second.
22 (Pause.)
23 MR. WILSON: Can you hear me now?
24 VICE CHAIRMAN BUDKA: We heard you 20 times with
25 the echo I think.

1 MR. WILSON: Okay. I'm turning the volume on
2 that way down.
3 VICE CHAIRMAN BUDKA: Perfect. That's perfect.
4 Thank you, Robert.
5 MR. WILSON: Thank you very much. If you can go
6 ahead and queue up my slides, please.
7 VICE CHAIRMAN BUDKA: You're all queued and ready
8 to go. Seven minutes, Robert. Thank you.
9 MR. WILSON: Okay. Good morning. I'm speaking
10 to you as a public safety agency telecommunications
11 manager from the very rural state of Wyoming. I'm proud
12 to say that communications interoperability is built into
13 the public safety culture of Wyoming. Individual
14 agencies out here often don't have the numbers of
15 personnel in remote areas to handle crisis situations
16 alone, so law, fire, EMS, transportation and many other
17 front-line responders routinely manage emergencies
18 cooperatively at the scene of the incident.
19 Though we continue to depend on government-owned
20 communications, especially in remote areas where suitable
21 comms aren't available, agency subscriptions to fast
22 commercial broadband are steadily increasing, leveraging
23 technology to serve our citizens better. So what does
24 this nationwide public safety broadband network have to
25 offer? I think these technical requirements are key:

1 First, grade of service, that is, better broadband
2 coverage. Second, interoperability and mobility,
3 including commercial networks. Third, public safety
4 priority as we just heard; and fourth, reliability,
5 availability and security, which are points left to other
6 panels, so I won't touch on them, but they are very
7 important.
8 The slide for grade of service, please. I break
9 grade of service topic into two parts, coverage and
10 speed. There's rural coverage challenges. The cellular
11 provider with the largest footprint in Wyoming provides
12 3G mobile broadband coverage to about half of Wyoming's
13 geography. That's not bad considering how sparsely
14 populated some areas are, but it falls far short of the
15 need of public safety agencies for voice communications
16 here.
17 Though the census may show no residents in an
18 area, citizens count on public safety agencies to provide
19 service to countless people who travel and enjoy
20 recreation in these unserved areas. They perform their
21 life-saving missions there.
22 Our legacy LAN mobile radio system can provide
23 fundamental voice comms with far better coverage than
24 commercial cellular gets, but it can't provide mobile
25 broadband, and to be cost-effective in rural Wyoming, the

1 nationwide network must provide sufficiently fast mobile
2 broadband service, and coverage should be better and
3 certainly not worse than commercial mobile broadband
4 offerings.
5 The second part of grade of service is broadband
6 speed. Typically current commercial 3G users experience
7 768K bytes per second download. That's about the minimum
8 for basic internet: staying connected, basic email,
9 simple web browsing and law enforcement records
10 management for example.
11 I was recently asked my opinion as to whether it
12 would be fruitful for FirstNet to offer agencies a
13 reduced bandwidth service of perhaps 50 to 100 K bytes
14 per second. Based on recent experience here, I'd say no.
15 I say that because our WyoLink LAN Mobile Radio System
16 already provides a low speed P-25 data capability at no
17 charge to agencies that choose to use it, and it's
18 perfectly adequate for applications like simple database
19 queries or automatic vehicle location reports.
20 However, we find smaller agencies have been
21 hesitant to invest the effort to scale down their
22 broadband applications to operate over this low-speed
23 link. Agencies want to use their unmodified applications
24 that are designed to run perfectly well on commercial 3G
25 networks, and this is a moving target. Speed

1 requirements are increasing as commercial 4G becomes more
2 common.
3 The next slide is on mobility and handover.
4 Public safety agencies, responder agencies, need cost-
5 effective interoperability and mobility, including on
6 diverse commercial networks. Considering the limited
7 FirstNet funding and the high cost of building a
8 completely segregated public safety radio access network
9 across rural states like Wyoming, innovative public-
10 private partnerships seem essential, and we've heard a
11 lot about that earlier today.
12 There's important provisions in Title VI of the
13 legislation about public safety communications in regard
14 to commercial networks and partnerships in general.
15 Section 6206 directs economic partnerships with existing
16 commercial mobile providers to speed deployment in rural
17 areas. It also provides for FirstNet to enter into
18 agreements with commercial providers to allow public
19 safety to roam onto commercial networks and gain
20 prioritization in emergencies.
21 Section 6211 provides for the FCC to adopt rules
22 if in the public interest to enable public safety
23 networks to roam onto commercial networks and gain
24 priority if some provisions are met.
25 Other sections provide for secondary users under

1 a leasing arrangement, and I'll do a quick quote here.
2 It says "between first responder network authority and
3 secondary user to permit access to network capacity on a
4 secondary basis for public safety services and the
5 spectrum allocated to such entity to be used for
6 commercial transmissions".
7 The next slide is on priority and QOS.
8 Provisions are needed for public safety precedence when a
9 network is under congestion, as was just said, and that
10 includes priority when roaming on commercial networks.
11 Exactly 10 months ago the NPSTC priority and QOS
12 work group started up, and over the course of many, many
13 web meetings and much email dialogue, I learned a lot
14 from the 30 to 50 diverse and sharp participants on that
15 work group. We ultimately achieved consensus for some
16 very controversial and complex issues, and I understand
17 you have a draft version, probably the same April 2 draft
18 version that's the last one that I've seen, and I draw
19 your attention to that as the technical advisory board.
20 Two key parts of that on the slide here are
21 responder emergency and immediate peril. Responder
22 emergency is a feature that today's typical radio systems
23 provide so that a responder can instantly report when
24 he's about to lose the ability to communicate normally,
25 usually because of physical jeopardy. Responder

1 emergency sets off high-profile alarms and takes the
2 highest precedence of network resources to urgently bring
3 the responders support and assistance.
4 A similar functionality is required for
5 responders as we move into broadband on the nationwide
6 public safety broadband network. But it needs to be
7 expanded beyond voice to include any application, such as
8 voice, video, data or whatever is around the corner.
9 And immediate peril. Immediate peril is a new
10 feature that was deliberated on by the NPSTC Priority and
11 QOS Group. It's used to indicate an immediate threat to
12 any human life, not just the responders. It's intended
13 to permit frontline personnel to responsibly escalate the
14 most vital data communications so they'll maintain the
15 minimum essential speed for the application despite
16 congestion, even congestion from other responders.
17 This should be most valuable under congestion in
18 the crucial first phase of a large multi-agency incident
19 as responders are just arriving but before any
20 intervention from an on-scene incident command system
21 comm unit leader for example. Overarching standards are
22 needed for appropriate use of this feature. They need to
23 be set nationally but routinely enforced regionally or
24 locally to discourage abuse.
25 And that concludes my remarks. I thank you for

1 the opportunity to give my input.

2 VICE CHAIRMAN BUDKA: Thank you very much,

3 Robert. Now we move to Roger Quayle.

4 MR. QUAYLE: Thanks, Ken. Can we bring up my

5 slides? Okay. As we've heard, the Interoperability

6 Board is required to base its rules on the LTE standards,

7 so in terms of priority and QOS on LTE, I'd like to look

8 first at the mechanisms or the toolbox that the standards

9 give us.

10 First of all, there are the PCC rules, which is

11 the QCI, which is the packet forwarding behavior, the

12 guaranteed byte rate and nonguaranteed byte rate bearers

13 and then allocation and retention priority, ARP, which is

14 really the user level priority. There are then Traffic

15 Flow Templates which are used to filter packets to

16 different bearers of different priorities depending on

17 the packet type or the application. And then finally

18 there's access class barring where groups of users can

19 completely blocked be from access to the network during a

20 major incident.

21 I'm not going to go into detail. These slides

22 are really just background. We're showing two users and

23 the QCIS that are available, the bearers, are really

24 those defined for the user, those available for the user,

25 as defined in the PCIF database. And then the Traffic

1 Flow Templates are filtering the different packet types
2 onto those bearers that the user is allowed.
3 So the challenges with LTE priority and QOS in a
4 public safety context. First of all, I think it needs to
5 be recognized that the QOS mechanisms in LTE were
6 developed without any thought of public safety needs
7 simply because the standards work predated what's
8 happening here in the U.S. with public safety.
9 But also they were developed without any real
10 commercial operator experience in QOS and the 3G
11 networks, so we really are breaking new ground here
12 taking LTE and its QOS into an application for public
13 safety where priority and QOS is absolutely essential.
14 So the challenge is how do you translate the mechanisms
15 that are defined in the 3GPP standards into a priority
16 scheme that's actually meaningful to public safety users.
17 One of the issues that we understand from having
18 similar QOS mechanisms on the network that we have for
19 New York City is that there has to be a sufficient
20 perceived difference between the different priority
21 levels given to users. Otherwise, that priority becomes
22 somewhat irrelevant.
23 The challenge we have is that -- and I'll cover
24 this in more detail on the following slides -- the
25 standards limit the degrees of freedom that we have for

1 the total number of users and applications for the
2 nonguaranteed byte rate data, and because LTE is
3 primarily a data network, that's a challenge.
4 So, first of all, on priority for voice, given
5 that longer term this LTE network is required to carry
6 public safety mission critical voice, and it is going to
7 become a very significant application, the standard
8 actually fits voice quite well because you define
9 guaranteed byte rate bearers for voice and then you use
10 the allocation of retention priorities to prioritize
11 users. You can also limit the maximum resources used by
12 voice so you don't completely squeeze out critical data
13 applications.
14 So the real issue with the standard QCIs is that
15 the first four QCIs are guaranteed byte rate, and
16 guaranteed byte rate can be very inefficient on a packet
17 based sheer channel network. You can very quickly run
18 out of capacity if you're allocating too many users for
19 guaranteed byte rates of relatively high levels.
20 And then you've only got QCIs 5 through 8 for
21 non-GBR and then one bearer QCI-9 for essentially sheer
22 channel applications. Now it is possible in the
23 standards to support up to 255 QCIs, so there's a
24 possibility of future standards work to use some of that
25 capability for public safety.

1 So operational governance issues, we think that
2 deciding who gets what priority is really a governance
3 issue to be addressed by the FirstNet authority. It
4 needs to be recognized that operational considerations
5 are probably going to require that local jurisdictions
6 can change priority in real time to deal with major
7 events or incidents.
8 The question of how QOS should operate in roaming
9 situations, and also the Interoperability Board needs to
10 be cognizant in writing the rules to take into account
11 that states that decide to opt out may have different
12 requirements and also to ensure that it doesn't preclude
13 the non-public safety uses which are allowed under
14 public-private partnerships.
15 So conclusions on priority and QOS, we believe
16 that the Board should regulate the mechanisms based on
17 the 3GPP standards and not the governance policies and in
18 doing so require the standard LTE priority and QOS
19 mechanisms, which I list here, also require excess class
20 barring, particularly with commercial users on the
21 network and other noncritical users. And as I mentioned,
22 consider proposals to 3GPP to add additional QCI
23 definitions. I see I'm running out of time, so I think
24 I'll skip the slides on grade of service and handover.
25 VICE CHAIRMAN BUDKA: Great. Thank you very

1 much, Roger. I open it up to the Board for questions.
2 Dereck or Diane?
3 MS. WESCHE: A question for Mr. Wilson on the
4 bridge. You talked about the need to get coverage in
5 your state and other rural areas where there is not
6 presently any kind of broadband coverage.
7 A question for you in the area of the scope of
8 our board. I think that's a very important issue. I
9 think one of the areas that the Board is trying to
10 wrestle with is how far do we go in that. Surely
11 FirstNet needs to address decisions on where to build out
12 the coverage. So my question for you is what would you
13 be expecting this board to be saying in that area about
14 how coverage should be expanded in rural areas and how
15 that affects interoperability?
16 MR. WILSON: Yes. This is Robert Wilson on the
17 phone bridge. My take would be the reality is that
18 subscriber agencies have a choice, and if they're given a
19 choice that has worse throughput or if they're given a
20 choice with less coverage, they're not going to use the
21 public safety network. They're going to stay with the
22 commercial stuff that they're starting to adopt now. So
23 I'd say as an absolute minimum the coverage and the
24 throughput needs to be as good or better than the
25 commercial alternatives. Does that answer your question?

1 MS. WESCHE: That helps. Thank you.
2 MR. ORR: Kind of a followup to Diane's question,
3 and I think as a Board, we've certainly discussed the
4 issue of I think scope like Diane just said and we heard
5 this morning. And I heard from a couple of the panelists
6 about coverage issues, capacity issues. Pat, I think
7 you brought up capacity issues and backhaul, and
8 something we're having to focus on is, as we heard this
9 morning, the statute discusses minimal technical
10 requirements for interoperability.
11 And so we've gone back and forth, and it's the
12 razor's edge of what is interoperability and what is the
13 technical requirements, and just as a matter of example
14 just to get people's opinion on this, let me just give a
15 couple of scenarios and just get your feedback on whether
16 or not you can consider this an interoperability issue.
17 In Example 1 -- and I'll give both of them out
18 and then you can answer them both. They're both simple
19 enough to contemplate. One is if I'm using two
20 subscriber units from the same manufacturer, and I'm
21 talking to you, Pat, outside of a building and everything
22 is working fine and let's say even the core network is
23 all part of the same manufacturer, and I walk into the
24 building into a fade situation and I lose the capability
25 to talk to you, did I just have an interoperability

1 issue, or did I have a coverage issue from a network
2 design perspective?
3 The second scenario is let's say you and I are
4 having a video chat, whether it's the same manufacturer's
5 products or a different manufacturer's products. So
6 we're having a fantastic video chat. Everybody starts
7 watching Netflix at once during our video chat, and our
8 video chat goes down because the network is now at
9 capacity or overcapacity. Did we have an
10 interoperability problem between each other, or did we
11 have a capacity issue on the network from a network
12 design situation?
13 And I just would like to get the panelists'
14 perspective on those two scenarios and whether or not
15 that's interoperability or is that operability and
16 network design.
17 MR. AMODIO: Yes. I think on the first one it's
18 a coverage issue. On the second one, it's an
19 interoperability issue. I firmly believe that maybe the
20 Board should consider like maybe urban, suburban, rural
21 type requirements, and I think you can have different
22 levels of service in those areas.
23 So my point earlier was maybe if you had a rural
24 requirement, minimum requirement for coverage and
25 capacity and you meet all the applications and all the

1 mission requirements for all the users and both coverage
2 and capacity, then you meet the interoperability
3 requirements for the people that are using in that area.
4 The reason I said the first one was a coverage
5 issue is you probably met all the requirements, but you
6 maybe didn't have coverage in the building and that
7 wasn't part of the requirement for the urban scenario.
8 MR. QUAYLE: A general comment. While I think it
9 might be seen as desirable to specify minimum coverage,
10 minimum building penetration, minimum sullage rights and
11 so on, I think it's a stretch to define those as
12 interoperability. Now there's this cute saying that you
13 don't have interoperability unless you have operability,
14 but I think you've got to step back and question whether
15 that's actually a logical statement.
16 I think the other dilemma is that the FirstNet
17 authority is not going to have enough funds to build out
18 an entire nationwide network, so they're going to have to
19 make tradeoff decisions, and I don't think unfortunately
20 the Interop Board can make those decisions in advance
21 because the Interop Board really doesn't have the
22 business model and the economic equation that FirstNet is
23 going to have.
24 VICE CHAIRMAN BUDKA: Thank you, Roger. Robert,
25 Scott, any comments?

1 MR. WILSON: I have a question, but nothing
2 really to add I guess. And this is Robert Wilson again.
3 My question would be does the Board or any of the other
4 participants have any insights -- I'd done a quote there
5 on my slide about mobility and handover from some of the
6 sections of the legislation that provide for a leasing
7 arrangement, and one of the clauses in there that I found
8 intriguing and I'm wondering how that's going to be
9 interpreted or used is when it talks about a leasing
10 arrangement between the first responder network authority
11 and a secondary user to permit access on a secondary
12 basis for non-public safety services.
13 And then it says "and the spectrum allocated to
14 such entity to be used for commercial transmissions".
15 What does that mean and where could that go?
16 VICE CHAIRMAN BUDKA: So we are looking at the
17 different roaming and mobility requirements that a public
18 safety user would experience on FirstNet. The statute
19 limits our requirements to the public safety broadband
20 network part of that equation, so our current
21 interpretation is to stick to that.
22 I just wanted to ask a question. So NPSTC has
23 been doing a lot of work on envisioning LTE and the use
24 of LTE by first responders and we heard some discussion
25 from Tom Sorley earlier today about prioritization and QOS.

1 There's a document out by NPSTC envisioning some
2 new ways of using the degrees of freedom that LTE does
3 provide for prioritization and QOS and using that to
4 provide functionality that's needed for first responders.
5 And we heard Robert talk about immediate peril
6 and also the need for jurisdictional controls. A
7 question about where the line for minimum requirements
8 should be set, especially in the event that many of these
9 features have not been specified yet in any standards
10 body, at least that type of level of control.
11 Roger, just curious what your thoughts are in
12 terms of what minimum requirements the Board should be
13 setting related to these specific behaviors.
14 MR. QUAYLE: Well, I don't have a perfect answer.
15 I think there is a dilemma in that when you look at the
16 priority and QOS defined in the LTE standards, it's
17 really not a perfect foundation for what public safety
18 requires.
19 VICE CHAIRMAN BUDKA: As a followup, is there
20 anything you would do now to perhaps limit creativity in
21 the interest of preserving interoperability going forward
22 in terms of creativity of developing that type of
23 functionality, testing that functionality?
24 MR. QUAYLE: Well, the Interop Board is required
25 by legislation to base its rules on 3GPP standards, but I

1 think we all recognize that, for example, mission
2 critical, push to talk group call voice still needs to be
3 standardized, and what I would advocate is that that be
4 done strictly within the 3GPP standards and not by
5 deviation into any other standards body or industry group
6 specific to U.S. public safety.
7 And also I mentioned in my slides the possibility
8 to define additional QCIs because the signaling allows
9 255. So that's something that can be done within 3GPP.
10 So I think that that limits the innovation, proprietary
11 innovation that might be a disadvantage to public safety
12 in the long-term. But I think also the Interop Board
13 should really limit what it does in terms of suggesting
14 future 3GPP standards work and write the rules so that
15 they are neutral to what needs to be done in the
16 standards and then have that standards work separately be
17 led by PSCR with support of the vendor community.
18 VICE CHAIRMAN BUDKA: Thank you very much, Roger,
19 and our thanks to Pat, Roger, Robert and Scott for your
20 contributions today. Thank you very much.
21 (Applause.)
22 MR. SHEPHERD: Thank you. So my name is Brian
23 Shepherd. I'm the Deputy Director of the Adams County
24 Communications Center, one of the waiver recipients, and
25 the Chair of the Security Working Group. I'm still

1 trying to figure out how I chaired this group as the
2 element of security in this network is pretty daunting to
3 think about, and there's a lot of people that know a lot
4 more than I do about that.
5 So I've been privileged to work with a lot of the
6 folks on this Board and have helped this work. We have
7 an excellent panel here. I think I'm really excited to
8 hear about the breadth of the knowledge that we have.
9 First off, we have Mark Adams. He is the
10 Director and Principal Architect for Network
11 Communications from Northrop Grumman. We have Dr. Mark
12 Althouse, a Technical Director, Mobility Mission
13 Management from the National Security Administration. We
14 have Tom Farley, Senior Systems Engineer from Raytheon,
15 and we have Matt Schnell, Supervisor of
16 Telecommunications for the Nebraska Public Power
17 Authority. So, with that, we will start with Mr. Adams.
18 So, Mark, please.
19 MR. ADAMS: Okay. I'll try to get my voice to
20 work here. I was at the Caps game rocking the red last
21 night. Unfortunately it didn't turn out quite the way I
22 would have had it turn out, but we're going to get them
23 Wednesday. Anyone from Boston, we can talk later.
24 Where I want to start first of all is just to
25 talk a little bit about the fact that FirstNet is going

1 to be a national critical infrastructure, and hardly any
2 day goes by when you're reading *Wall Street Journal* or
3 any other major newspaper in the United States or across
4 the world that some kind of information about a cyber
5 attack or some type of attack on a critical
6 infrastructure occurs. In fact, today's news is about
7 the Iranian oil industry, who had to disconnect from the
8 internet because they were under attack. Last week we
9 had some major news about some of our state and local
10 agencies as well as state-based agencies who had been
11 attacked.
12 So it's hardly a day in the newspaper where
13 there's not something about that. The frequency and
14 severity of the attacks is increasing, and for this
15 network, security is a comprehensive issue. It's larger
16 than any individual protocol like LTE or any individual
17 standard, and it's larger than any individual product or
18 vendor product that can be brought to the table. It's a
19 comprehensive issue. The risk is larger than that.
20 Northrop Grumman has significant experience in
21 managing very large critical national infrastructure
22 assets for agencies at every level of government,
23 starting with public safety all the way up through
24 national security type agencies, and the scope and scale
25 of this network is one which is going to require the type

1 of expertise that we and others across the industry can
2 bring to this problem. This is a much different problem
3 than public safety is used to dealing with with LAN
4 mobile radios, which tend to be individually disconnected
5 from each other. Security of FirstNet requires a
6 holistic approach, and I'm going to bring out some issues
7 that we put together, and I just wanted to give you some
8 background before I got started on that.
9 What I want you to consider as you look at
10 security for this system is that there needs to be an
11 enterprise level architecture. If you think about LTE
12 and how it works, this isn't your traditional wireless
13 network. Essentially when you hit the RAN and the data
14 turns into IP traffic all the way out at the RAN, it's a
15 completely flat infrastructure, so it essentially can be
16 managed like we manage major enterprise core networks
17 today.
18 And a lot of the security issues that are out
19 there already have a lot of industry standards and
20 capabilities and tool sets that are out there for
21 managing networks like this. The issues that are out
22 there that might be unique really reside mostly on the
23 handsets and what happens on the handsets: things like
24 applications, how are applications managed, what can
25 applications do and what do you need to do to protect the

1 particular information privacy and other things that you
2 might not necessarily think about when you're a
3 commercial user.
4 As I said earlier, security needs to be
5 comprehensively designed in. There needs to be access
6 controls built in. You have quality of service and
7 access that's going to require some significant work in
8 determining how you make those two things work together.
9 There needs to be malware detection and virus
10 detection across the entirety of the network, all the way
11 from locality to the national scale. We believe there
12 actually needs to be a FirstNet SOC, security operations
13 center, that there will actually have to be someone who's
14 responsible to define the security standards. That does
15 not mean the implementation happens at just the national
16 level. Obviously you have to have security protocols at
17 every locality at every part of the network, but it needs
18 to exist.
19 And there also needs to be a centralized
20 applications platform. Not every application on this
21 network will have to be secure, but some of them will.
22 If you think of a SGES application, for instance, that
23 would reside on a device that is going to read SGES data
24 and provide it to a user, well, first of all, that user
25 has to be identified as someone who can access that kind

1 of information, it needs to be logged that the access
2 occurred, and it needs to make sure that that information
3 could never be misused or somehow remain on the device
4 after that interaction occurs.
5 So application and application security needs to
6 be very, very key to this network. Let's see. I'll go
7 to the next slide. And this just is a drawing that we
8 put together to try to give you a sense of the three
9 major components that we think need to be considered as
10 it relates to security. Those three major components are
11 on your right on the network, and that is a subscriber
12 management clearinghouse, really an identity management
13 platform.
14 We do not believe that security can be properly
15 implemented on this network without an identity
16 management system that is interoperable across the
17 entirety of the users in the network. If you are going
18 to be able to manage the security and know who's using
19 the network, know what access they have, know where
20 they've gone, know where they are allowed to go, then you
21 have to have a common identity platform, a common way of
22 identifying who's using the network and how and when
23 they're allowed to use it.
24 I already mentioned the need for a SOC. We
25 believe that there is a place for a nationwide SOC, which

1 will then work with the localities in the regions that
2 might also have security implementations on their side.
3 And then I already mentioned the importance of
4 managing applications and having an enterprise
5 application hosting common apps that can provide these
6 critical infrastructure type applications in a secure
7 fashion. Thank you.
8 MR. SHEPHERD: Thank you very much, Mark. Next
9 up is Dr. Althouse.
10 MR. ALTHOUSE: Thank you. Thanks for inviting me
11 to participate in this important event. Within our
12 shores the physical safety and security of our nation
13 really depends to a great extent on the work of our
14 emergency responders, and so we're happy to share the
15 lessons that we've learned in developing security
16 standards for the wireless mobile communications and the
17 infrastructure for that that we've done for our customers
18 in the federal government and hope that it will help
19 achieve a user-friendly, secure, reliable and
20 interoperable wireless communications capability in times
21 of crisis and for daily operations.
22 A few quick words about NSA and our mission. NSA
23 leads the U.S. government in cryptology that encompasses
24 both signals intelligence and information assurance
25 products and services. So the signals intelligence

1 mission is collecting, processing and disseminating
2 intelligence information from foreign signals. That's
3 not what I do.
4 I'm on the information assurance side, and what
5 our mission is is to prevent foreign adversaries from
6 gaining access to sensitive and classified information.
7 So we're charged with protecting national security
8 information and information systems in accordance with
9 National Security Directive 42.
10 And my specific piece is to deliver secure mobile
11 solutions using commercial platforms, to provide anytime,
12 anywhere access to classified networks using a defense
13 in-depth approach which layers commercially available
14 security products and services to protect devices and
15 infrastructure while maintaining that rich user
16 experience.
17 So that last part, using the commercially
18 available equipment all the way through, is really a new
19 thing for us. We used to build our own stuff. And I
20 think that change to doing all of this with commercial
21 will really help the Interoperability Board.
22 You've already heard about the threats and kind
23 of the daily nature of things getting in. There's been a
24 lot of information out on that and steady adversaries,
25 and that's really informed what we do and our approach to

1 security in all of the systems that we recommend,
2 including mobile wireless communications.
3 So given that nature of the attacks not only from
4 nations, states, terrorists, criminals, everybody out
5 there that's getting into this space, if you can agree to
6 a common reference architecture and a set of commercial
7 security standards, it will go a long way to assuring
8 responders are able to communicate among themselves and
9 with state, local, tribal and federal users without the
10 need for common handsets or devices.
11 So getting into the technical aspects. There are
12 a number of basic security layers to consider. One of
13 the simplest is data in transit. We use multiple layers
14 of encryption on that, and one of the focuses is making
15 sure that the device communicates only with the
16 enterprise. And it really leverages the enterprise
17 security and the strength of that and all of that
18 investment in the enterprise network to the greatest
19 extent possible rather than to try and put that out in
20 the end point, and that way the enterprise can manage the
21 information and the access.
22 Let's see. I've got just one slide that -- yes,
23 there we go. In this reference architecture, there's a
24 number of -- five actually -- primary interfaces or
25 points of interoperability that have security elements.

1 Just starting off, they're numbered on there,
2 it's kind of hard to see, but the radio interface
3 protocols, and usually there is encryption and
4 authentication pieces in that, they're from, as
5 mentioned, 3GPP but other wireless networks as well. For
6 instance, we use the WPA2 and WiFi, and because that can
7 be enterprise-controlled, you can get some significant
8 protection from that. Using an enterprise core and
9 controlling some of the other cellular elements in that
10 radio layer, you can get some goodness out of that as
11 well.
12 The outer encryption layer of VPN, some of the
13 things that we use in our system: IP Sec, Suite B, which
14 is a set of algorithms. Then an inner layer of
15 encryption can be linked to voice. We use SDES or DTLS
16 SRTP data, again another Suite B, IP Sec. For browser-
17 based things, SSL, and we're looking to get some
18 standards put in place for SSL VPNs to make that a little
19 bit more robust and uniform.
20 The application protocols, a lot of that right
21 now is proprietary, and these are what you're going to
22 have in your individual departments. Interoperational
23 requirements are going to be fairly different. So there
24 might be some interoperability that you can get out of
25 that, but it's not maybe as crucial.

1 Management protocols, and there is something that
2 for mobile device management we see as a critical element
3 and an area where there are not standards yet, but they
4 are being developed. Maybe not specific to the client
5 and the enterprise piece, but getting a way to express
6 what you need out of that, the amount of control that you
7 need in the device and how it should be enabled.
8 There's also public key infrastructure and key
9 management infrastructure. There's standards for that as
10 well, and that kind of has to back up a lot of the
11 security pieces that you've got because they're going to
12 be based on certificates.
13 There's a number of other areas. I've got them
14 in my script but can't get to them. Just one final
15 thought. I believe the recently passed legislation and
16 the Board, your board, and the FirstNet can really bring
17 this together and provide the nation with a way to avoid
18 some of the legacies of 9/11 and Hurricane Katrina where
19 we couldn't communicate and really get the national
20 standard for the hose couplings.
21 MR. SHEPHERD: Thank you. Next up, Tom Farley
22 with Raytheon.
23 MR. FARLEY: Good afternoon, and I appreciate the
24 opportunity to be here. In the interest of time, I'm
25 probably going to just touch on a few of the slides. We

1 know broadband service is here, and so basically the
2 implication is that users are going to be able to do the
3 things that they do back at the office that they can do
4 mobile.
5 Since LTE is an IP-based design, it means that
6 the security vulnerabilities and flaws of IP are going to
7 be inherited. Industry can expect the attack trends will
8 follow similar to what we've seen in computer networks
9 but exponentially faster as these type of attacks have
10 been practiced.
11 Just to make a few points. Roughly 16 percent of
12 users have adequate security on their mobile devices, and
13 that wasn't including tablets and e-readers and things
14 like that. So that number is significantly lower, so we
15 know that the risk is there.
16 Some of the interoperability points most people
17 seem to be in line with. I guess one of the things that
18 the Board is going to have trouble with is defining the
19 scope and how far down that goes. One of the things that
20 I've heard here is maybe we can't control what users do,
21 but at least the user devices, so I've broken it up into
22 the transport, the access devices, end point devices,
23 core services and LTE management.
24 The LTE transport comprises of all of the
25 equipment used to expose and control the data path. In

1 FirstNet, this is going to be a physically distributed
2 network across defined regions. Some of the issues that
3 we've heard before is compatibility matrix, so maybe if
4 the Board doesn't actually specify the compatibility
5 matrix, they can say that one from FirstNet will be
6 defined.
7 Some of the questions about the configurations on
8 security, the actual answers aren't so much important as
9 the fact that they're conveyed all the way down in a
10 specification for people to implement. There's a few
11 points at the end that I'd like to get to since some of
12 this has been covered.
13 LTE access devices include hot spots, USB modems,
14 4G sleeves. They're prone to direct attacks. They can
15 be lost or they can be stolen. I know some of the major
16 vendors of 4G today have actually had some compromise of
17 these hot spots, so that leads people to actually jump on
18 them and use those data paths illegally or without
19 access.
20 Some of the things that could be implemented to
21 change this can actually impact user interoperability.
22 So the way a user logs in, the way they access these
23 devices, if they're changed, it could cause a denial of
24 service to users if they're trying to access it,
25 especially in emergency situations or when they go to

1 different areas than what they're used to.

2 End-user devices will undoubtedly be the largest
3 domain for vulnerabilities and attack points. Equipment
4 is subject to user exploration and/or controls, so
5 configurations must be maintained. Possible issues here
6 are the typical ones: worms, trojans, viruses, packet
7 snippers. The fact that users can touch configuration
8 invites tweaking or what is known as jail-breaking of
9 devices.

10 To limit the damage, end-user policies and
11 security awareness training is a must, and forcing
12 software configurations and providing a means of patch
13 management and software version control is crucial. So
14 that goes along the lines of a SOC or a NOC function.
15 Vulnerability assessments of these end-points for
16 compliance and configuration of software loads and
17 reporting of tampering evidence will prevent some of
18 these attacks.

19 That's something I haven't heard yet is
20 vulnerability assessments, so that's a key part of all
21 these interfaces here is looking at that security
22 posture.

23 Back-end core services is defined as global
24 applications available to end-users, such as SMS,
25 location-based awareness, things like that, since they're

1 not defined, we're not really sure what all is going to
2 be there, but I've heard data and video streaming, which
3 are all high-level data applications that the users are
4 going to want to see. If they're not available
5 immediately, at some point, they are going to be and
6 they're going to want them added, web components if
7 applicable.
8 Applications are subject to traditional Layer 7
9 attacks, so IDS, IPS, firewall type things are the normal
10 things that I would expect to be in there. And again
11 vulnerability assessment for these back-end services is
12 critical for making sure that something doesn't happen.
13 Implementing a metatagging solution with
14 filtering can be used as a form of digital rights
15 management to ensure data is not accidentally released.
16 That's one of the points that I'll touch on here in just
17 a second.
18 In most cases, we already know that the hackers
19 and malicious users are on the inside, so perimeter
20 security is no longer sufficient. LTE management will be
21 done from the LAN or remotely, and the LAN is usually
22 connected to the WAN in some way, so there is typically a
23 back door. Remote access machines in many cases are
24 personal machines that are used with VPN tunnels and
25 multiple interfaces on those devices can cause split

1 tunneling. So even though I come in with a VPN, I can
2 access the device through BlueTooth, through the WiFi or
3 other devices or other interfaces to gain access to the
4 network.
5 Policy also almost never requires a remote access
6 device to be reported if it's lost or stolen because it's
7 not something that they track. It's not an asset that
8 was purchased, and so they're not required to report it
9 stolen. Some mitigations above risk are to limit
10 concurrent network interfaces so that only one is
11 available at a time and provide strict hardware/software
12 policies. Let me get down to the takeaways here.
13 So, in closing, documented configuration
14 guidance, communicative process and procedures, vendor
15 selection capability matrix, and periodic vulnerability
16 assessment and penetration testing are all the important
17 things.
18 A few other points that I wanted to make is that
19 we can put all the security that we want into it and make
20 it super tight, but during a crisis, one of the things
21 that you may want to look at is the ability to drop that
22 security and how fast you can do that, and so if
23 something happens.
24 The other thing I heard Pat earlier talk about,
25 DHS deployments. It sounded just like the military to

1 me, you know, Com Ops, Common Operating pictures,
2 situational awareness. And so the military has the same
3 problems when they go overseas and they have to
4 interoperate with other countries, you know, how do they
5 do those communications.
6 And then as far as the actual spec, along the
7 lines of dropping the fence, maybe you don't have to
8 specify what it has to do, but maybe you can specify what
9 it won't preclude that it will do. So PKI, user
10 federation and things like that, even though it may not
11 be required initially, you can say that it won't preclude
12 the use of those kinds of things. Thank you.
13 MR. SHEPHERD: Thank you, Tom. Next up, Matt
14 Schnell from Nebraska Public Power.
15 MR. SCHNELL: Thank you, Brian. I'm going to
16 take security and wrap it into what we've done in
17 Nebraska in a partnership and go through the security and
18 that partnership and what we've done with both.
19 That partnership was formed between Nebraska
20 Public Safety and the utilities in Nebraska. The
21 partnership was formed to ensure all first responders,
22 public safety and utilities can seamlessly communicate
23 with each other during emergencies, disasters, special
24 events and normal work that requires coordinated
25 resources. So the presentation that I have is centered

1 around the experience that Nebraska Public Safety and
2 Nebraska utilities have gained from a shared LAN mobile
3 radio communications system. Our system also shares a
4 common monitoring system and a combined backbone network
5 that carries all the traffic for this radio system for
6 both voice and data on the system.
7 The joint network between public safety and
8 utilities uses multiple security methods, combined to
9 protect the interoperability system. The different
10 methods that we use match the requirements of the
11 combined system. So, on the public safety side of that
12 combined network, we use MPLS for the network part of the
13 security, and on the utility side, we use what I would
14 call private path circuits where we just take circuits
15 and map those up without going through anything else.
16 The combined network is in a ring configuration
17 that provides the most robust system for reliability, for
18 bandwidth requirements, survivability and cost
19 efficiency. We are able to combine these security
20 methods along with VLANs to keep our system secure, and
21 we did that without having to do major changes to the
22 network to get these systems to work.
23 Customer touch points are tied in with firewalls
24 to make sure that the data exchange is secure. Inside
25 the system we use a combination of passwords, access

1 lists, advance system keys and encryption to set up the
2 allowing the users to access the information that they
3 need. This provides us with multiple layers of security
4 to access the user information. The security methods
5 that we use here do meet all the vendor requirements for
6 the system that we're trying to protect.
7 Along with the technical part of this, I wanted
8 to touch on the process because I believe that the
9 process goes hand in hand with the technical part of any
10 type of system. So the security requirements that we
11 have in our system were developed through a collaborative
12 effort between public safety and the utilities. A
13 combined public safety and utility team was tasked with
14 setting up all the security measures on the system.
15 The security network set up the security
16 requirements along with the system on how they monitor it
17 and how they make changes to that system. Along with
18 that, a users group made up of all of the system users
19 developed and recommended the security needs of the users
20 on the system, and these recommendations were then passed
21 on to the security network team along with the owners of
22 the system to determine what the impact was going to be
23 to the system and what risks were out there as we looked
24 at introducing these things. All approved recommendations
25 were then implemented by the combined team.

1 System documentation, which is always a concern
2 when you're trying to secure things, was looked at by the
3 network team, and then we went ahead and took sensitive
4 information and put it to the people on a need-to-know
5 basis only.
6 Security networks and user requirements were
7 developed together to determine what impact each will
8 have on the other system. Security network teams need to
9 ensure as we did that data requirements like system-to-
10 system collaboration, user-to-user collaboration and grid
11 modernization are all addressed. As with our current
12 radio system, the areas of coverage, reliability,
13 survivability, latency, security, risk management and
14 network capability are critical to both public safety and
15 utility operations and service.
16 Public safety, security as well as reliability
17 and priority needs are both very similar for us as for
18 public safety. Both groups have critical priority
19 information as well as less vital secondary information.
20 An example, as we move forward into the data world,
21 public safety may need a live video stream from a crime
22 scene situation that is a high priority while a utility
23 may have a functionality that is also a high priority.
24 Both examples need the appropriate security and network
25 capacity to ensure that both get through when needed.

1 Both groups also have high priority safety requirements.
2 From our experience in Nebraska, it takes a
3 public safety and utility team effort to understand each
4 group's critical needs, set the correct priorities for
5 user information, determine the best security measures
6 and establish the system requirements that will ensure
7 critical traffic is available when needed. The team
8 concept has been integral in our success in Nebraska on
9 this combined use system. We have shown public safety
10 and utilities not only can work together but must work
11 together to meet all of our requirements for first
12 response.
13 If we can make these things work together in
14 Nebraska, technology will just provide us the means to
15 share the critical networks. So the last slide I have on
16 here is actually kind of the two groups that play vital
17 parts in Nebraska right now in our security network
18 requirements. These groups are made up of both utility
19 and public safety people. Thank you, Brian.
20 MR. SHEPHERD: Thank you. Thank you to all the
21 panelists for your time and effort in this endeavor.
22 First off, I'll open it up to questions from the Board.
23 Dennis?
24 MR. MARTINEZ: So, Mark, you used the word
25 holistic, which we certainly agree with. One of the

1 challenges we have really is to define the boundaries of
2 scope. 3GPP clearly has a well-defined security
3 architecture, and clearly it's a very small piece of the
4 whole security architecture. So, if we look at layering
5 and/or adjacent security systems and we look at minimum
6 technical requirements, can you offer any advice, areas
7 of inquiry that we should look into? So adjacent and
8 layered on top of that minimum 3GPP baseline?
9 MR. ADAMS: Well, I guess in the interest of
10 time, I will reiterate what I think is the most important
11 issue, the difference between a commercial network and
12 what you're trying to do with FirstNet, and that is
13 properly identifying users, properly giving them
14 appropriate access to the locations in the network that
15 they have rights to use at the priorities that they have
16 rights to use those applications.
17 And then the second thing would be really
18 thinking through the whole issue of what does an
19 application do on the device, what happens to the
20 information when it's done being used. Does it reside,
21 does it stay, what might the threat be to a particular
22 application or to a particular device if someone were to
23 in fact deliver malware via an email message into that
24 device. Would it somehow have access that it doesn't.
25 As was stated by the gentleman from Raytheon, Tom, only

1 16 percent of people have proper protections today on
2 their mobile devices, so we cannot have that obviously in
3 FirstNet. So those would be the two issues, identity and
4 application security.
5 MR. MARTINEZ: Mr. Farley, could you also --
6 MR. FARLEY: Yes, I guess the only other thing
7 I'd mention there is that we can identify the users and
8 we can identify their access, but if we don't identify
9 the level of data that's being ran through the network,
10 then you need all three things to allow access.
11 And so I mentioned metadata tagging, which I
12 didn't get a chance to touch on it too deeply, but one of
13 the things that the military has always fought with is
14 they didn't mark their data originally and natively. And
15 so they have this big task to go back and relabel
16 everything, and so if the parameters aren't put into the
17 specification to do so or allowed to do so, then we're
18 missing a piece. So all three of those will get you the
19 access control that you need and protect the need to know
20 that people are talking about.
21 MR. SCHNELL: Dennis, I'd like to add one thing,
22 and that is the security around the people that have
23 access to all the information, where it goes across the
24 network, this gets into your provider part of that and
25 that those individuals that have access to that, that

1 they meet the secured requirements of the users out there
2 that have that data going across the networks.
3 MR. ALTHOUSE: I guess I kind of look back to the
4 aspect of enterprise control and really derive that from
5 there. Now the enterprise in terms of crisis response or
6 a large emergency, you know, you may have a fire
7 department or a police department, they've got their own
8 enterprise, various state agencies and federals, when
9 they come together, you have to have a mechanism to merge
10 that into one enterprise so that they can interoperate
11 and correctly allow them to have access to the right
12 amounts of data and get back to their own enterprise.
13 But then there has to be some pooled content I
14 think going forward, so setting up those access
15 mechanisms that are uniform across the various
16 enterprises so that you can get collaboration just beyond
17 being interoperable. So, if I take my device and I go
18 into the neighboring state, I can get access to the
19 network and through that network get back to my home
20 enterprise. But really the aspect of when you have to
21 collaborate can be very difficult if you don't have that
22 nailed down right.
23 MR. AZZI: Yes, and the same theme, I'm going to
24 ask the question a little bit inside out and maybe take
25 it to an extreme place to encourage some critical

1 thinking. If we define our work to be limited to the LTE
2 network itself, which to me is the physical aspects of
3 it, if we limit it to interoperability, which would
4 preclude things like the fundamental security of the
5 source code within a network element and take all the
6 other security functions, many of which are very proper
7 and appropriate and things you all articulated and stay
8 silent on it as an Interoperability Board and rely on
9 FirstNet to define those practices, would we be missing a
10 key opportunity that you would look to us and say shame
11 on you for not addressing this?
12 MR. ADAMS: I think that I wouldn't say shame on
13 you, but I wouldn't be happy because to me -- I was going
14 to say this earlier and I didn't, security --
15 interoperable security is a matter of trust and trust
16 means that you need to have as you described it a trust
17 relationship between the way that people access data.
18 Now I understand that you need to not over specify to
19 FirstNet, because as was mentioned earlier, there are a
20 lot of aspects of the business model and other things
21 that need to be dealt with.
22 However, to be able to declare some type of
23 intent, that there would be some -- say FirstNet security
24 plan that is instituted and executed at a FirstNet level,
25 even though some of the implementation would happen at

1 the locality, or at the regions, to have a standardized
2 approach to all of these security related issues, even if
3 you're just saying use industry standards.
4 Because as I said, this network is not all that
5 different than any other government enterprise network.
6 It just happens to have LTE attached to the end of it.
7 So a lot of the standards that already exist out there
8 can be leveraged and called upon to implement this kind
9 of network. But you do have to keep in mind the
10 differences between a commercial network and what
11 FirstNet is, which is a government network.
12 MR. ALTHOUSE: I think that your LTE core and the
13 RAN associated with that gives you -- it is your
14 transport, and it certainly provides some security
15 services, and I think within your scope that you can
16 delve into those a little bit further.
17 I think it would probably be incumbent upon you
18 to say, all right, that is only part of the picture of
19 what the operational capability of a first responder is.
20 And so noting those other security layers which are key
21 to interoperability and collaboration and really making
22 sure that what you lay down for the LTE part will not
23 interfere or break or limit any of the other flexibility
24 in solving the rest of the security layers.
25 And kind of leave that as open as can be so that

1 you can go to the commercial enterprise and say I need
2 something that will do this for me and try and maybe
3 point towards some of the other standards of those
4 layers.
5 MR. FARLEY: Yes, I would just like to say -- and
6 I wrote it down earlier -- and again scope is hard to
7 define here. You know, where does it stop. Does it stop
8 at the edge. But it doesn't make any sense to build a
9 transport that the users can't really use. So one of the
10 things that I mentioned was maybe you can't define the
11 specification now, but you can at least not preclude it
12 from being added into the future.
13 So again how FirstNet is going to be used
14 initially may not end up how it is being used in five
15 years. So try to have some kind of insight into what
16 that might be, and how those users are going to do it.
17 So we mentioned digital rights management, and
18 that is probably the end all item for document or data
19 security, and even though we can't implement it now -- it
20 is very expensive, and it is hard to manage, and we have
21 key management and all that stuff -- at least we can look
22 at the system and say, all right, we are not going to
23 limit digital rights management out of the system.
24 MR. SHEPHERD: I had one question. I had never
25 really thought about this, and I believe -- and who was

1 it. Tom, I believe you brought it up. In instances
2 where you don't want to decrease security, and you said
3 that I realize that there could be an incident where you
4 want as much information as you can possibly get. And
5 that may include people that aren't really trusted on a
6 day to day basis, but they have information. So can you
7 just expand on that a little bit about how you would go
8 about decreasing your security, and yet maintain -- you
9 know, it is kind of a dichotomy, but I think it is
10 important to address.
11 MR. FARLEY: Yes, so PKI was mentioned as one of
12 the requirements, and so you build all your network
13 around PKI enforcement, but at one point, you know, if it
14 is a wartime situation, or a crisis situation, you have
15 to allow that PKI not to go through.
16 If the PKI system breaks, you don't want people
17 dying because your system was built to enforce that
18 standard. So you have to have some kind of mechanism, or
19 some kind of bypass to enable that security almost at the
20 push of a button.
21 So how that gets designed in, you know, that is
22 another question, the technical enforcement, but the fact
23 that it is in the specification, and you can do that, I
24 think that is what is important.
25 MR. ALTHOUSE: You can go to as Tom said, you can

1 build in bypass mechanism, and it is like the battle
2 override switch. Okay. You take some risks, and you
3 flip up that red thing, and throw the switch, knowing
4 that when you do that, you lose certain access.
5 You may not be able to get to certain parts of
6 the enterprise, or certain information, but it allows you
7 to get around maybe broken parts of the security
8 mechanisms that are there that would otherwise prohibit
9 you from talking.
10 We have a thing like that in our pilot system
11 where if you need to make an emergency phone call to 911,
12 that breaks our security boundary, and so you can do it,
13 but once that has happened, you have to get the front
14 reprovisioned before you can get back into the secure
15 enterprise. So it is something like that.
16 MR. ADAMS: I think the important thing is that
17 what they describe is not decreasing security overall.
18 You are not opening the system up. You are bypassing
19 certain structures or protocols for short periods of
20 time. But the system is still protected, and only those
21 things that are approved for those types of bypasses will
22 work.
23 MR. SCHNELL: And you can set those up ahead of
24 time, and it is not much different than the LAN mobile
25 radio system that we have in Nebraska. We have encrypted

1 channels on there that are just for that so that nobody
2 else can hear them. But in the time of an emergency, we
3 have alternatives for that group to get off those
4 encrypted channels into an area where they use a shared
5 channel, and where they can talk to anybody out there,
6 and anybody else can hear them, and then when they are
7 done, they go back to their encrypted, but those things
8 are set ahead of time.
9 MR. SHEPHERD: I have been given information by
10 Chuck to go over a little bit, and so I think we have
11 time for one more. Dennis, you had a question?
12 MR. MARTINEZ: What if a fundamental security
13 flaw was detected in the 3GPP standards? What would you
14 advise that person to do, and therefore what might you
15 contemplate as the requirement of the technical
16 standards?
17 MR. ALTHOUSE: Obviously, you feed back to the
18 standards body that information, and try to get them to
19 fix it, but that is going to be a long term solution. So
20 when faced with something like that, you look at the
21 security layers that you do have, and there is no overall
22 prescriptive process.
23 But you just say, okay, this bit is broken, and
24 do I have sufficient other layers or mechanisms at hand
25 that I can enforce or maybe strengthen that will mitigate

1 the risk that I now face because that element has a flaw
2 in it, and I have to live with it until it is fixed in
3 the standard, and the industry brings out patches to
4 accommodate it.
5 MR. AZZI: Yeah, I would just like to add that I
6 think that you kind of already do that with device end-
7 to-end VPN encryption, and so you are already providing a
8 tunnel within a tunnel of the transport.
9 So if the encryption of the transport is broken,
10 then you have to add another layer, or use a different
11 layer of security to do that. And so you feed that spec
12 back, and hopefully that is a fiber patch or something
13 that gets fixed quickly.
14 But if it is in the specification design, then
15 that probably -- it could be lack of testing for
16 something that was -- you know, maybe you are trying to
17 do something that it wasn't designed to do.
18 MR. SCHNELL: You know, on the other side, the
19 user side of that, I think in this technical -- and even
20 though it is not a technical type comment, mitigation
21 strategies need to be set up in there so that there is a
22 user trust, that when something like this does happen
23 that the users have trust in the system that it will get
24 fixed, and they will be notified, and there is a
25 mitigation strategy to go with that.

1 MR. ADAMS: So this is where I was talking about
2 this SOC concept, and this is where this kind of thing
3 would reside, right? We have these certain weaknesses or
4 we have gotten -- we have had some malware attacks on the
5 West Coast, and the East Coast should be looking for that
6 particular malware.
7 I mean, these are the kinds of functions that
8 this organization would do. They would also interface
9 with your national security type groups that are managing
10 all the critical infrastructure in the U.S., and are
11 looking for these patterns in other parts of the
12 networks, in other networks, and they can share
13 information and look for these risks that are out there.
14 As well as failures in particular technologies,
15 which are also shared, and things, and it is not only LTE
16 that has risks. There is other parts of the IP
17 infrastructure that have or will have risks of having
18 failures or holes in them.
19 MR. SHEPHERD: Thank you, gentlemen. Thank you
20 all for your time and your effort. We sincerely
21 appreciate it, and I have enjoyed learning from you.
22 Thank you.
23 (Applause.)
24 VICE CHAIRMAN BUDKA: Thank you. My name is Ken
25 Budka, and I am with Alcatel-Lucent, and I am Vice Chair

1 of the Interoperability Board. In our discussion about
2 interoperability today, we have heard about QCIS, AARP,
3 SRTP, SDES, EAP, PLMNIDs, 3GPP, PTCRB, OMA, S1, X2, X5,
4 PKI, et cetera, et cetera.
5 First responders have a much more profane
6 definition of interoperability. Three simple words. It
7 just works. And it just works no matter where first
8 responders are, no matter what vendors supply their user
9 device, or their software. No matter what vendors supply
10 the network infrastructure, as long as the user is
11 authorized, it just works.
12 LAN mobile radio networks used by our nation's
13 first responders today fall far, far short of this level
14 of interoperability that is conveyed by these three
15 simple words.
16 And I think that it is clear today that we are
17 beginning a journey. This is maintaining and creating
18 that level of interoperability, and we are taking steps
19 today, but these are steps that will continue to be made
20 over time. This is a path that we set on after our
21 nation's response in the wake of the terrorist attacks
22 over a decade ago, and these attacks laid bare some of
23 the flaws in our nation's public safety communications
24 systems.
25 Responses to hurricanes and other natural

1 disasters in the years since have continually reinforced
2 the need for fully interoperability communications across
3 Federal, tribal, State, and local agencies, and secondary
4 users.
5 The FCC's adoption of long term evolution as the
6 common technology platform for public safety broadband
7 communications was a significant step forward toward it
8 just works, and establishment of FirstNet also a giant
9 step forward toward it just works.
10 There are many steps more to come, including the
11 important work that has brought us here today together,
12 and as we continue this work, we would like to call your
13 attention to the Public Safety Docket 12-74.
14 This docket was established to solicit comments
15 and additional material that will be helpful to the Board
16 in its deliberations, and we urge and need your
17 participation in this public safety docket.
18 On behalf of the members of the Technical
19 Advisory Board for First Responder Interoperability, we
20 extend our heart felt thanks to our distinguished
21 panelists, guests, and attendees. Thank you very much
22 and good afternoon.
23 (Whereupon, at 12:53 p.m., the workshop in the
24 above-entitled matter was concluded.)
25 //

REPORTER'S CERTIFICATE

WORKSHOP TITLE: Technical Advisory Board for First Responder Interoperability, Public Workshop

WORKSHOP DATE: April 23, 2012

LOCATION: Washington, D.C.

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

Date: April 23, 2012

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