TRANSCRIPT OF PROCEEDINGS

IN THE MATTER OF:)
)
CRITICAL INFRASTRUCTURE &)
INFORMATION COLLECTION)

Pages: 1 through 123

Place: Washington, D.C.

Date: April 13, 2010

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

FEDERAL COMMUNICATIONS COMMISSION

IN THE MATTER OF:)
)
CRITICAL INFRASTRUCTURE &)
INFORMATION COLLECTION)

TW-C305
FCC Building
445 12th Street, S.W.
Washington, D.C.

Tuesday,
April 13, 2010

The parties met, pursuant to the notice, at 9:03 a.m.

BEFORE: JEFFREY GOLDTHORP

ATTENDEES:

JEFFREY GOLDTHORP, FCC
JAMES ARDEN BARNETT, JR., FCC
COLLEEN BOOTHBY, Levine Blaszak, Block & Boothby
MARECK MASTER, Telecondia Technologies
JIM BUGEL, AT&T
JOE SANDRI, FiberTower
HAROLD SALTERS, T Mobile
TOM TAVARES, Expirix
JORGE MAGANA, Director, Level II Communications
DAVID KEECH, Frontier Communications
MARK ADAMS, Cox Communications
BRETT KILBOURNE, UTC
RICHARD WOUNDY, Comcast Cable

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

2 (9:03 a.m.)

3 MR. BARNETT: Good morning. My name is
4 Jamie Barnett. I have the privilege of being the
5 chief of the Public Safety and Homeland Security
6 Bureau for the Federal Communications Commission.
7 Thank you so much for joining us today. We appreciate
8 you taking time to be here, particularly in light of
9 what I thought might be transportation issues that you
10 may have faced because of the nuclear security summit
11 being held today, although I have to tell you that my
12 commute from Northern Virginia for the last few days
13 has been better than it's ever been. I think a lot of
14 people have stayed out of the city.

15 I also want to thank our panelists for
16 taking the time to be with us today and sharing their
17 knowledge and expertise with us, and we look forward
18 to hearing from you.

19 It seems fitting that we are having
20 discussions today about protecting and ensuring the
21 nation's critical communications infrastructure while
22 members of 47 other countries are gathered here in
23 D.C. to discuss security issues.

24 Communications are essential to the safety
25 and security of the government representatives and

1 dignitaries who traveled here, the community and those
2 who protect them, and we are acutely aware of how
3 critical it is for us to gain a better understanding
4 of the survivability of existing networks and explore
5 potential measures to reduce our vulnerability to
6 failures of network equipment or severe overload
7 conditions in emergencies. This is especially true as
8 Americans increasingly rely on broadband services for
9 so many aspects of their lives, including public
10 safety and national security.
11 Although we are not here just to talk about
12 broadband technology and communications, it's
13 important for us to note that advanced broadband
14 communication technologies have dramatically changed
15 the lives of Americans and others around the globe by
16 enriching the way they communicate and receive
17 communication and information.
18 The internet, which relies on broadband
19 communications, is part of our critical information
20 infrastructure, and is particularly vulnerable to
21 malicious attack. Included among these are Legacy of
22 the underlying technologies not originally designed
23 with security in mind. The lack of central authority
24 for enforcing security policies, dependency on
25 security measures that should be taken by millions of

1 end users, some more technically sophisticated than
2 others, and I would include myself in that, and the
3 ease of duplication and deployment of attack tools
4 using the internet itself. Clearly, then, we should
5 not have a false sense of security or competence with
6 regard to the survivability and survival of our
7 broadband communications infrastructure.
8 A successful attack on communications
9 networks can affect all end users that rely on
10 broadband networks. Our base of communication
11 services is in the midst of an historic migration for
12 traditional network technologies to internet-based
13 technologies, and IP telephony has penetrated American
14 households at a staggering rate. In the years to come
15 the existing 9-1-1 network will undergo its own
16 transformation to this new generation of technologies.
17 This migration of critical emergency services will
18 bring with it legitimate concerns about vulnerability
19 and security. A successful cyber attack on such a
20 network, for example, could severely hamper the
21 ability of our first responders in even knowing about
22 and responding to emergencies.
23 With this in mind, the FCC is interested in
24 finding the best ways to obtain and analyze data
25 received from all broadband service providers

1 concerning network and service disruptions. Our
2 experience in receiving and analyzing data for
3 communication providers concerning disruptions in
4 their networks has proven effective in providing us
5 early warning of potential attacks or instances on the
6 nation's existing communications net works.
7 This information allows us and our partners
8 in the communication industry to mitigate adverse
9 effects and expedite restoration of service. Our work
10 is based on a sector-wide view of communication
11 outages and allows us to spot industrywide or carrier-
12 specific reliability and security concerns.
13 We use this information in conjunction with
14 DHS and communication providers to produce long-term
15 improvements to communications reliability and
16 security. For example, we recently observed a
17 statistically significant upward trend in the number
18 of events affecting wireline carriers. We worked with
19 industry to establish a team of experts to examine the
20 data in closer detail, and developed a set of
21 recommendations. In the intervening months we have
22 measured a 28 percent decline in this category of
23 outages. In other instances we have noticed
24 concerning trends in the data of specific providers.
25 With this information in hand we can meet with

1 communication providers, discuss the situation, and
2 develop a plan for addressing the issues.
3 This expertise and methodology carries over
4 very well to the world of internet reliability.
5 However, we currently lack the necessary data to study
6 these issues. With similar information from broadband
7 and internet service providers, the FCC and its
8 federal partners could work with industry on sustained
9 improvements to internet-based infrastructure. The
10 application of this data-driven process would help
11 improve the reliability of broadband infrastructure,
12 which is vital to our security. We are currently
13 examining the best path forward to obtain this
14 information, and that's why we are here today.
15 I would like to thank you again for being
16 here, for your interest in this important topic, and
17 now I'd like to introduce and turn this over to our
18 chief of the Communications Systems Analysis Division,
19 Jeff Goldthorp. Jeff.
20 MR. GOLDTHORP: Thanks you, Jamie, and thank
21 you all for being here this morning. Thanks to those
22 in the audience and those on the webcast and joining
23 online.
24 Why don't we begin today just with
25 introductions and I've talked to the panelists

1 beforehand and asked if each of you could just tell us
2 who you are, your title, and just a word or two about
3 your duties.
4 Mark, why don't we start with you?
5 MR. ADAMS: Mark Adams. I'm the corporate
6 senior director for reliability and quality at Cox
7 Communications.
8 MR. KEECH: Dave Keech. I'm assistant vice
9 president of engineering with Frontier. I have
10 responsibility for our ISP operations at this time,
11 and have previously managed our knock operations.
12 MR. MAGANA: Jorge Magana, Sr. Director,
13 Level III Communications. I run the voice and soft
14 switch and circuit switch infrastructure and knock.
15 MR. MASTER: I'm Mareck Master with
16 Telecondia Technologies. I run the government and
17 sector business. Spend a lot of time at AT&T prior to
18 that as well, and I have experience ranging from
19 networks that do basically administrative type
20 services, what is today the networks contracts for the
21 federal government, all the way up to specialized
22 networks for specialized applications.
23 MR. BUGEL: Jim Bugel with AT&T. I'm
24 assistant vice president of public safety and homeland
25 security which encompasses emergency preparedness,

1 cyber security, and network reliability.

2 MR. GOLDTHORP: Thank you all again, and we

3 will have two panels today. The first panel this

4 morning has to do with survivability and resilience of

5 communication networks. What we want to learn is

6 where in communications networks today, particularly

7 broadband networks, we would be most likely to find

8 things like single points of failure, those things

9 that we tried to avoid in years past, where redundancy

10 exists in those networks, and where traditional types

11 of maintenance and provisioning procedures, grooming

12 procedures can result in conditions where redundancy

13 had existed before where it may no longer exist,

14 particularly physical diversity.

15 Then, finally, we want to explore the effect

16 of surges in traffic, particularly at the edge of the

17 network, on the ability of networks to provide

18 services, so, for example, think of the snow event

19 that we had here in D.C. back in February, and the

20 large number of folks that were working from home

21 during that event. We want to talk a little bit about

22 what your observations were during that event, and

23 what steps communication providers take to manage

24 traffic flows during events like that.

25 And then when we get to the second panel,

1 that will be more about information collection, and
2 the kinds of things that the Commission has looked at
3 in the past, and maybe ought to be looking at in the
4 future, but I'll save more detailed remarks on that
5 until we get to that panel.
6 But let's start this panel, which is more
7 about physical layer survivability and resilience, not
8 so much logical error but physical error, and looking
9 not just at next generation communications but also
10 current generation communications because broadband is
11 a word that we us now, and we tend to use in the
12 context of IP but broadband, high capacity transport
13 networks have been around obviously for years, for
14 sometime, and these networks have been around.
15 We obviously have had networks in place and
16 have taken steps over the years to try and make sure
17 that the number of instances of single points of
18 failure, places in the network where a single failure
19 could result in a catastrophic or a large-scale
20 outage, that those instances or those places in the
21 network are minimized.
22 So, what I'm wondering is as we move from
23 Legacy technologies to broadband technologies, do we
24 expect that there will be more instances of single
25 points of failure or do we expect that as the

1 communication technologies themselves sort of take on
2 a more distributive nature that the instance of single
3 points of failure will start to diminish over time
4 just by virtue of the fact that the technology will be
5 tending to drive us there.
6 So does anybody want to lead off with that?
7 MR. MAGANA: We can start by talking about
8 the grooms that you mentioned at first. Typically,
9 the grooms from a Level III perspective is typically a
10 migration not necessarily to strand any customers or
11 capacity. It's basically looking at the network, our
12 network from an access perspective, and then as things
13 come to term or if there is a cheaper way to provide
14 diversity, that's when we'll do a groom, or you know,
15 for a better term, migration.
16 But typically a migration or a groom never
17 isolates a customer, and it should be transparent to a
18 customer usually done through a maintenance window,
19 coordinated through whatever access providers we may
20 be partnering with.
21 MR. GOLDTHORP: On that grooming topic, does
22 anyone else have a -- I think, Jorge, what you're
23 driving at there is sort of the question of grooming
24 traffic or moving traffic around maybe from circuit to
25 circuit and to deal with puts and takes, as needed.

1 Anybody else want to take that up? And then we'll
2 come back to the single point of failure issue. But I
3 have a follow-up question when we're ready. Go ahead.
4 MR. KEECH: Pursuant to that, I think one of
5 the things that we have run into some issues with is
6 two points: Notification from carriers, Frontier, in
7 particular, leases a number of intestate, interoffice
8 facilities from a number of different carriers, and
9 maintenance activity notifications are important,
10 obviously, so that we're aware of the situation and
11 take proactive action to prevent some sort of outage
12 if we're aware that an activity is going on which
13 could impact it.
14 But secondarily, a follow-on activity from
15 that is that once that groom is done the activity of
16 reviewing records to make sure that we haven't
17 eliminated what had previously been a redundant
18 circuit, because perhaps a circuit was moved to a
19 fiber which is now shared within a facility by another
20 carrier with whom we have what we thought was a
21 redundant circuit, and it no longer is. So one of the
22 things that we're doing is focusing on, and our
23 maintenance activities, the follow-on action to ensure
24 that redundancy and reliability that had previously
25 been evident prior to a maintenance activity is in

1 fact still there subsequent to maintenance activities,
2 particularly by carriers with whom we have business
3 relationships.
4 MR. GOLDTHORP: So this is a good thread
5 because I want to distinguish between physical
6 diversity and logical diversity. So are you able when
7 you're doing what you're describing, David, are you
8 able to know that you're maintaining physical
9 diversity or logical diversity or both?
10 MR. KEECH: That is directly dependent upon
11 the quality of the records that we have both within
12 our own systems as well as those that have been
13 conveyed to us as part of the ordering process, i.e.,
14 the DLRs associated with those circuits.
15 It's much easier to determine whether or not
16 we have physical redundancy because of those types of
17 records, although depending upon the degree to which
18 those are automated in the system that may be a matter
19 of simply looking something up online as soon as we
20 get the maintenance notification. It may in fact be
21 as difficult as sending that notification out to a
22 field engineering organization in the region and
23 asking whether or not there is any potential impact or
24 concern with this transfer.
25 At the logical level, I think the

1 implementation of practices consistent with ANRAC and
2 other recommendations, dual egress feeds, for example,
3 dual routers, dual power supplies at the logical level
4 make that considerably less likely that a physical
5 groom is going to impact at the logical level with
6 redundancy, at least we have not seen such so far.
7 MR. GOLDTHORP: It would seem to me that at
8 the logical error you would have better data available
9 to you because the circuit level data is available in
10 circuit databases, right, whereas physical layer data
11 often, my understanding, that oftentimes you would
12 have to go to plats or, you know, cable records, but
13 maybe that's not true anymore. Maybe those records
14 are automated as well.
15 MR. KEECH: It directly gets to the point I
16 made earlier about how automated those records are.
17 MR. GOLDTHORP: Okay, yes. So how automated
18 are they?
19 MR. MAGANA: You know, as you're partnering
20 with -- there is going to be Type II circuits to get
21 out to the access world, and your records may indicate
22 one thing, your design layout record, your DLR may
23 indicate one thing, but it can be completely dependent
24 upon the access provider's records as well, how
25 accurate they are, and typically during the groom

1 process, you know, this is not something that takes
2 place over, you know, just a few days, it's typically
3 a highly coordinated event where typically from a
4 Level III perspective it's about 30 to 45 days in
5 planning before execution to get those design layout
6 records correct and make sure that -- make sure that
7 the disconnect is, you know, from the old circuit to
8 the new circuit is not impactable to the customer, and
9 then to have the new design layout records be, you
10 know, the most accurate ones.
11 And sometimes because it is highly
12 coordinated times you have to actually send out field
13 services techs, you know, from different companies,
14 whoever you're partnering with, to physically audit
15 all of the circuits and all of the connections and
16 those sorts of things.
17 MR. GOLDTHORP: We're drilling down pretty
18 deep on this one, but this is -- it gets very
19 interesting because any given circuit is probably
20 going to be composed of multiple -- the supply train
21 can be pretty long, right? You know, you can go
22 through multiple carriers to get from one end of the
23 circuit to the other carrier, and multiple SLAs
24 intervening, I'm guessing, and so how do you, for
25 example, how do you when you're dealing with a groom

1 like this is there a need to coordinate with
2 wholesalers or suppliers of capacity downstream,
3 further downstream than your immediate supplier of
4 bandwidth, and how does that work?
5 MR. MAGANA: Well, you have to you have to
6 coordinate with everyone all the way on down the line,
7 and that's where the audits come in, that's where you
8 physically check everything before the activity takes
9 place. There is no other way to get around it without
10 potentially being impacted.
11 MR. GOLDTHORP: Maneck?
12 MR. MASTER: Just something to add to the
13 grooming process. The other piece to this thing that
14 makes the job very difficult is when you are sitting
15 in a network organization and you're worrying about do
16 I have diversity of the pig pipe, if you will. You
17 worry about all those things and you can sort of get
18 it all done the way we are describing it, you know,
19 whether it's in the system or you get it done
20 manually, et cetera.
21 I think the other part which is actually
22 somewhat more difficult is sort of up the change.
23 There were customers who are using pieces of that
24 bandwidth, if you will, and sometimes relatively small
25 pieces of the bandwidth, and maybe those customers are

1 going to be impacted by the grooming process, that you
2 have done things that were diverse before are no
3 longer diverse now. Things that should have been
4 kept, you know, with X degrees of separation are no
5 longer that way, and it's very difficult, I think, in
6 a company where you're sort of doing this, sometimes
7 at least on a weekly basis if not a daily basis,
8 you're grooming the network because that's what is
9 required of you if you are the network provider, to
10 kind of worry about all the effects at the customer
11 end of the service, and I think that's sort of the
12 full supply chain because as a customer, you know, all
13 these things, I think, should not bother what I bought
14 from the company, and yet they do, and it's very
15 difficulty to automatically keep track of all these
16 pieces of the pie.
17 MR. GOLDTHORP: Jim.
18 MR. BUGEL: Yes. While I agree with
19 everything that's been said, and certainly has covered
20 a lot of territory, there is another dimension and
21 that is the capital efficiencies and the cost
22 efficiencies which are dealt with in this entire
23 process. So that is one other element that is
24 involved when you provide these services and how you
25 design these services.

1 MR. GOLDTHORP: Could you be more specific,
2 Jim? What other kinds of issues that you --
3 MR. BUGEL: You can build to a level that
4 basically strands capital in a certain area of your
5 network which is inefficient, capital inefficient.
6 You can build to a level that basically takes a
7 portion of your network beyond acceptable cost
8 structure, so those are the areas that these -- that
9 as they design and grew, those were also elements that
10 are also considered in this whole equation.
11 MR. GOLDTHORP: So you have to engineer
12 capacity and spend for the build before you actually
13 provision service, is that what you mean, before
14 everybody is buying capacity, right?
15 MR. BUGEL: Yes, I don't know if there is a
16 lot of people here at the table that actually go and
17 buy things before they get the capital improvement
18 done.
19 MR. GOLDTHORP: All right.
20 MR. BUGEL: So, yes, it has to meet the
21 requirements that are set by --
22 MR. GOLDTHORP: I mean your engineer --
23 MR. MASTER: I think the point is that the
24 companies are trying to deploy the capital in the most
25 efficient way to run the business. They are not

1 necessarily deploying capital so that, you know,
2 certain parts of the network will have more resiliency
3 except in the cases where there is a market for that
4 kind of resiliency that somebody wants to pay for. I
5 think that's sort of the tension between the user and
6 the supplier in the communications marketplace that
7 has been around for decades.
8 If a user says, well, I don't want my
9 circuit to be down, but can I give you 10 percent
10 more, it may be that the capital requirements to do
11 what you're asking for may be 10 times, not 10 percent
12 more, and you're not willing to pay 10 times more, so
13 you're very frustrated that, you know, you've got to
14 pay that much more and you don't understand it. From
15 the network provider's point of view, you know, not
16 too many people even if this particular customer was
17 going to pay you 10 times more, not too many other
18 people would pay you, so how do I spend capital in a
19 way to put bigger pipes out there in places where I'm
20 not sure there is a big market for that?
21 I think that's sort of the issue I think
22 that you're touching on.
23 MR. ADAMS: I agree with everything that's
24 been said. I think that, going back to the single
25 points of failure question, we design our networks

1 both from a broadband and a voice perspective to high
2 availability standards. There are things that can be
3 done to validate and find out where those points of
4 failure are, which is a reliability engineering design
5 for reliability, where you could actually model your
6 network and then you know where your high failure
7 points are, and then you engineer those out. That's,
8 you know, designed for reliability methodology which
9 we're big on.
10 On the physical logical error you can
11 actually do capacity modeling as well, so where your
12 fail links at a time you see where that traffic goes,
13 which we do that as well. So that when things do fail
14 you know which circuits are being highly utilized, and
15 then you try to engineer those out of the network. So
16 those are some of the things that we're doing to
17 ensure high availability for all our services.
18 MR. GOLDTHORP: What else is done to --
19 Maneck, do you want to --
20 MR. MARTIN: I actually want to go back to
21 your question, which is, as we go from now to
22 broadband do things get better or worse, et cetera?
23 MR. GOLDTHORP: Okay.
24 MR. MARTIN: Right? And let's kind of think
25 of it philosophically. I have a very large networking

1 infrastructure out there, and I want to get a very
2 small piece of bandwidth data, whatever you want to
3 call it, through that network. The network is
4 damaged. The network is congested. But what I'm
5 looking for amounts to .0000X percent of the total
6 network. I'm somehow able to find this bandwidth and
7 get it through with the right kind of mechanisms,
8 right?
9 Now I say, no, I want to increase, so I'm
10 thinking about, you know, some kind of a packet, some
11 kind of a text message, some kind of whatever it is
12 that somebody is trying to get through. It doesn't
13 mean the network is more resilient. The network is
14 the network, but what I was trying to get through was
15 a very small piece of this thing.
16 Now you're saying, no, I want as OC12 across
17 the network that is maybe the same network with the
18 same damage with the same kind of congestion, and I
19 want to get that on sort of a continuous basis, right,
20 so it's not a packet kind of thing, I want like an
21 OC12 circuit end to end across the country.
22 You have the same capacity totally
23 available. What you're looking for now is no longer
24 this tiny fraction of bandwidth that's available, but
25 a pretty big chunk. So if you start looking for

1 bigger and bigger chunks and want to see how that gets
2 through, I think inherently that's not going to happen
3 in the same timeframe. If nothing else has changed as
4 the network capacity grows over time and a decade from
5 now the network is 100 times more capacity rich than
6 it is today, then, you know, looking for a bigger
7 chunk at that time may be equivalent to looking for a
8 small chunk now.
9 So I think there is a question in my mind
10 about do things get worse if I just go to broadband
11 tomorrow and I'm looking for a bigger chunk of
12 capacity, and wanting a guarantee on that, if you
13 will, or wanting a high probability of success on
14 that, if you will, compared to looking for a very
15 small, narrow bandpiece. I think it gets worse.
16 MR. GOLDTHORP: I guess the thing that I
17 would push back with is sort of the premise that I see
18 fading too, okay, but for a different reason maybe,
19 and that is that at least in principal broadband
20 networks are based on IP technologies and protocols,
21 and in a pure sense these were designed to be very
22 resilient. You know, they were originally designed to
23 be very, very resilient.
24 And what I wonder when I ask the question
25 about distributed technologies, and really there is --

1 I kind of asked the question a little bit backwards,
2 or brought up the point a little bit backwards because
3 the concern I have is that you --
4 MR. MASTER: You were talking about physical
5 layer, but anyway go ahead.
6 MR. GOLDTHORP: When you're talking about IP
7 you're definitely talking network layer, right. So
8 now I'm talking about network layer.
9 So as we move now from more of a purist kind
10 of internet environment to an environment where
11 autonomous systems are getting -- are bigger and now
12 encompass much bigger asset bases and traffic is moved
13 around within using things like MPLS technology, which
14 is more like a virtual circuit technology, do we need
15 to be more concerned about things like reliability
16 because, you know, we're not talking about necessarily
17 as resilient a network -- now I'm talking network
18 layer -- resilient a network layer as we had been
19 years ago? Is that an issue that comes to your mind
20 as something that could lead us down a path of being
21 more vulnerable?
22 MR. MASTER: Depends on which part of the
23 network you reside in. I would say it's hard to argue
24 that the sort of old network before there was MPLS in
25 the backbone was fundamentally less resilient than the

1 MPLS backbone today.

2 If I looked at, for example, you know, the

3 old AT&T network, it was like 100 plus pads to get

4 from one end to the other, I could always use those.

5 I chose not to use those from an economic perspective

6 of capital deployment perspective or whatever, but if

7 I had an issue I had 100 pads to get through or 100

8 plus pads to get through.

9 So I think the MPLS regime does make things

10 more efficient. I'm not sure it sort of creates a

11 whole layer of resiliency because at the end of the

12 day if you don't have the physical capacity out there

13 because it's been impaired in some way, whether it's a

14 cyber plane or a physical thing, it doesn't matter how

15 many logic circuits you want to build on top of it,

16 you can only build as much as the physical capacity

17 allows you to do. So that's sort of what I'm trying

18 to get to.

19 MR. MAGANA: From a core network

20 perspective, there is capacity within the core

21 network, our core network say. The points of

22 congestion seems to be getting on the network. The

23 capacity to get on the -- you know, you can use the

24 surface street to highway analogy where, you know, you

25 can have a 12-lane highway, you don't necessarily

1 build a 12-lane surface street to get to the 12-lane
2 highway.
3 So once you get to the core network the
4 capacity is there. It's at the end points, it's at
5 the edge as we go to broadband which will create the
6 congestion points.
7 MR. KEECH: I would agree with that, yeah.
8 If you adhere to, accept a design standards, 50
9 percent fill, et cetera, you know, any competently
10 designed core network will survive significant
11 physical layer failures at the logical level. I think
12 it is a capacity issue. How do I get to it? And
13 that, because of the economics question that was
14 raised earlier, is definitely an issue of the best use
15 of capital in a limited capital environment.
16 MR. MANANA: I think the technology is
17 there. I mean, it's capable of high liability. I
18 think one of the challenges are as you implement these
19 new technologies people tend to go through a learning
20 curve which may result in a lower glare of liability
21 than something that you've had in the network for five
22 years. So I think part of the challenge is how do you
23 avoid that learning curve as you deploy new
24 technologies that become even more thought tolerant,
25 so I think it's the human element that we also really

1 need to focus on.

2 MR. KEECH: One more thing. We're probably

3 talking about congestion in the Tier II, Tier III

4 markets, you know. I think when you're talking about

5 the metro cities where, you know, I'm sure there is

6 various metro rings, you know, represented here, but

7 once you get out to the Tier II, Tier III markets

8 that's where the congestion points -- that's where

9 broadband is not necessarily as available, that's

10 where the congestion will take place as we go through

11 the next phase which is to provide broadband out to

12 those markets.

13 MR. GOLDTHORP: I'm not just talking about

14 congestion when I was talking before about say MPLS.

15 Maybe this applies, at least in my mind, to ethernet

16 as well, maybe not, but it's more that we went forward

17 with a model that sort of internet-based technologies

18 are fundamentally more resilient just because, you

19 know, you lose an asset you basically route to the

20 next router. You know, the networking technology is

21 designed for resiliency, and designed to be tolerant,

22 and to the extent that then we are applying sort of

23 more virtual circuit-type technologies, right, to IP,

24 are we somehow minimizing the resiliency that comes

25 with the technology, and is that something to be

1 concerned about?

2 MR. MAGANA: I don't know that we minimize

3 the resiliency. I mean, we go through -- from a Level

4 III perspective we are constantly going through loss

5 of redundancy analysis and, you know, time to repair

6 and those sorts of things. You know, we do operation

7 reviews to look at our network to see how it's

8 performing those sorts of things.

9 What you're talking about, I think, is a lot

10 of capacity management, traffic management, those

11 sorts of things. You know, we built that into our

12 network so at the core, you know, that's where we have

13 the most resiliency. As we start to get out to the

14 edge is where it gets a little more difficult to

15 manage.

16 MR. GOLDTHORP: Yes, I suppose the advantage

17 in newer I'll say circuit-based or virtual circuit

18 technology is that run on IP Is that you can at least

19 now talk about implementing quality of service

20 features, right, for certain IP-based services that

21 before on a pure IP-based network were not as

22 available, right, so there is some advantage to that

23 from a resiliency standpoint, right.

24 Okay, another topic I wanted to touch on on

25 single points of failure is DWM technology, or WDM

1 technology, sorry, I got the D and W mixed up, WDM
2 technology. And as wavelength division multiplexing
3 technology is moving into the network and the pipes
4 get bigger and bigger and the multiplexing
5 technologies are terminating more and more traffic,
6 are there concerns there?
7 Just like when DOXES were introduced years
8 ago, you know. Now we have these large boxes in the
9 network terminating traffic. What are the kinds of
10 issues that you see from a resiliency standpoint as we
11 introduce those technologies into the network?
12 MR. MAGANA: Well, I think the obvious is in
13 areas where you may have some collapsed rings due to
14 some geographical challenges and those sorts of
15 things, but those we also try to engineer out as much
16 as possible. There may be a large ring that has a
17 small span that may ride on a collapsed ring which
18 we'll try to identify or engineer out or manage around
19 that. Some of the limitations may be right of way,
20 some of the limitations may be geographic in nature
21 where, you know, maybe the fiber goes from underground
22 to above ground, those sorts of things.
23 But typically we should know where all of
24 those collapsed rings or single points of failure from
25 a network perspective are, and then either have a plan

1 to manage around them or have a plan to eliminate them
2 from the network.
3 MR. GOLDTHORP: anybody else?
4 MR. KEECH: I think from our experience the
5 wavelength division multiplexing hasn't brought any
6 issues with directly related to reliability other than
7 that you're packing more data onto a single pipe.
8 And getting back to the original point I
9 made about redundancy and making sure that when
10 traffic is groomed you know that your high bandwidth
11 pipe isn't in the same facility, same conduit, same
12 sheath as your redundant egress circuit. If it goes
13 down, whether it's on wave division or it's a sonnet
14 level circuit, you're still out in that context.
15 You're just not passing as much traffic in a smaller
16 pipe versus a larger pipe.
17 I don't think we've seen any issues directly
18 related to the advent of wave division multiplexing in
19 the network as a result of, you know, the concept of
20 that technology itself.
21 MR. ADAMS: I would agree with that as well.
22 I mean, and I think it goes back to solid design
23 practices, right, make sure you engineer your networks
24 to eliminate or minimize those points of failure as
25 David and others talked about.

1 Secondly, I think adding on the physical
2 limitations of -- you know, we try to avoid single
3 points of failure as a design practice as well, but
4 there are certain cases where there may be no choice,
5 right, due to geographical or physical or right-of-way
6 considerations. So again, you know, we take efforts to
7 minimize the potential risk to those failures but in
8 some cases you can't completely eliminate them.
9 And then if you get completely on the edge,
10 if you're looking at small commercial businesses, you
11 know, from a physical perspective you have to look at
12 their business requirements. They may not need a high
13 availability circuit, and they may not be able to
14 afford to actually pay for a redundant or a diverse or
15 a new circuit for that diverse, they just don't need
16 it, right. It could be a nine to five type circuit.
17 So all of those things come into pay as well.
18 MR. GOLDTHORP: Switching gears a little bit
19 now -- Maneck?
20 MR. MASTER: I don't think a WDM kind of
21 concentration adds anything, you know, to the
22 resiliency being less, whatever, the reliability being
23 affected because if you had not done that you're just
24 going to light up some more glass on the same cable
25 and put some more boxes, so in fact if you look at the

1 component reliability of all of these parts that you
2 would have had to put together, and then compare it to
3 their liability of deploying it with one WDM box,
4 chances are you actually increase the reliability of
5 what you're doing.
6 The problem I think that you're trying to
7 touch upon is what I will call a reconstruction. You
8 know, if you have an event and now you need to find a
9 better re-route, now you've got a cross-section of
10 traffic that you've got to find a re-route for, and
11 you know, so if you have designed the network right
12 surely single points of failure I don't think are
13 going to cause you a big problem, but even duplex and
14 triplex failures shouldn't really cause you much of a
15 problem if you designed the core network correctly.
16 It's the access pieces, as people have alluded to,
17 that you're going to run into all kinds of issues and
18 that's independent of whether you've deployed WDM or
19 not, I think.
20 MR. GOLDTHORP: Yes, you won't see this
21 technology used as much in the access network that's
22 for sure. It's more of a core network technology.
23 MR. MASTER: But you have this technology
24 deployed in certain networks now for 8-10 years, even
25 in thin-line networks that are specialized, and we

1 really haven't seen much of a problem caused by that
2 particular technology as opposed to other things like
3 physical cable cuts or whatever.
4 MR. GOLDTHORP: Your point, you know, I was
5 thinking, your point that you just made about, okay,
6 if it's not all going to bundled up in the same
7 terminal and in the same fiber on the same strand,
8 it's just going to be multiple strand in the same
9 sheath, and you're going to have multiple terminals
10 and more stuff to break. although the strands are
11 probably, you know, if there is a cut there is a cut
12 and they're going to take them all out, but it's
13 really in the terminal equipment, and if you've got
14 more stuff in there to fail, then there is something -
15 - I have to think about that. That's a good point.
16 Sort of classic reliability theory. The more stuff
17 there is to fail the more like it is going to be to
18 fail, right. Okay, good, thank you.
19 Let me switch now on these same two topic
20 areas, sort of the transport redundancy and diversity
21 as well as single points of failure. We haven't
22 really talked much about best practices or voluntary
23 type initiatives that might help us move this forward,
24 and I'm wondering if anything has any thoughts to
25 share given what we've talked about already in that

1 area. What are some things that could help improve
2 the situation?
3 MR. ADAMS: I think the Addis-type forums,
4 the National Reliability Steering Committee which is
5 an Addis forum, is a good committee. Its task is to
6 basically look at outages and look for ways to improve
7 the reliability of the overall network. I'm part of
8 that and it's a good forum. I think ANRAC, the best
9 practices that were developed a couple of years
10 through ANRAC 7, you know, there is a lot of knowledge
11 in those best practices on ways to design and operate
12 your network, and those are definitely, I think,
13 successful, as well, you know, required in the SEC
14 outage reporting module to specify if there was a best
15 practice that could have avoided that situation. You
16 have to put that in the report.
17 I think raising the awareness and getting
18 more participation in those would be a good thing for
19 more industry partner, so I would definitely encourage
20 expanding those types of programs.
21 MR. GOLDTHORP: Jim.
22 MR. BUGEL: Yes, we completely agree. I
23 mean, if you look at the best practices there is 800
24 plus best practices. I believe the majority of them
25 are focused on TDM network. So you know, expanding

1 that best practice work out into broadband or internet
2 and cyber is probably the right direction to go.
3 MR. KEECH: I would agree. I think any
4 service provider that ignores that wealth of knowledge
5 that has been collected and presented does so at their
6 own peril, and ultimately we are driven by the
7 expectations and demands of our customers in order to
8 improve the network to provide the service levels that
9 they require and expect, whether they be high-speed
10 internet users, small residents, or whether or not
11 they be small, medium office or large enterprise
12 customers. They all have certain set of expectations
13 and in some cases we have service level agreements
14 with those customers that we have to meet, and the way
15 we do that is to implement the best practices
16 associated with the wealth of knowledge that has been
17 gathered by the various committees.
18 MR. BUGEL: I would agree with that, and it
19 helps us develop some rigor around our SLAs and, you
20 know, in turn we also have what we call SLOs, which is
21 service-level objectives that aren't necessarily based
22 upon a contract with a customer but we want to use
23 best practices to minimize any impact to our
24 customers, and so we measure those things internally,
25 and those recommendations obviously help. If they

1 could be expanded, we would encourage that.
2 MR. MASTER: Jeff, just one more thing.
3 This may be beyond the legal reach of the Commission
4 maybe, I don't know, but the lawyers here they can
5 answer the question better, but as you go to this
6 global broadband concept, I mean, we've sort of taken
7 it for granted that we understand how the FCC report
8 outage work and all that good stuff, but really we're
9 are laying a global infrastructure, and there is no
10 such thing that the undersea cable operator has to
11 kind of report outage to somebody, et cetera.
12 So there is a movement going on in the IEEE
13 Communication Society to get all the cable operators
14 to figure out how these best practices and learning
15 sort of mutually from other peoples' events, et
16 cetera, would be helpful to all, and it's a challenge.
17 It's a challenge, but I think that would be another
18 thing to think through because when you're looking at
19 the global broadband, it isn't just, you know, getting
20 out into your access POP that's going to do it. You
21 don't know where the servers are located. You don't
22 know, you know, what you're looking for is, right. It
23 may be in India, China, anywhere else. So you need to
24 have the undersea and global infrastructure out there
25 so that your internet is -- you know, your broadband

1 is going to be functional, not just having the
2 physical capacity in the United States.
3 MR. GOLDTHORP: what do you suggest would be
4 a good forum for that to take place if it's not
5 already happening in IEEE or some other forum?
6 MR. MASTER: I think, you know, Luis has
7 been involved in a little bit of that and maybe she
8 can talk about that a little bit more later, but I
9 think it require a legal framework that doesn't quite
10 exist.
11 MR. GOLDTHORP: And international framework?
12 MR. MASTER: International framework, and we
13 think there are some things that Louis has discovered
14 through her studies for one of the government clients
15 where the FCC does have some authority over some of
16 these things. But typically, for example, let's say
17 there is a cable with a cablehead that resides or
18 touches the United States, the FCC has some legal
19 authority to do something about that.
20 Typically what the FCC appears to have done,
21 and I'm not an expert on this thing so I'm far
22 overreaching my capabilities here, but it never
23 stopped me before, but I think what the FCC appears to
24 have done and look at it from a commerce and economic
25 perspective will that make sense for that cable to go

1 in and grant the authority for that landing as opposed
2 to look at it from maybe resiliency or other kinds of
3 areas, and certainly I think there is some leeway
4 there that the FCC can choose to adopt.
5 So we can talk some more about that, but I
6 think that could be another important thing to look
7 at.
8 MR. GOLDTHORP: We've talked a little bit
9 about best practices and how important they are. One
10 thing I wanted to touch on real quick and then
11 something else in just a second. Somebody mentioned
12 SLAs, and I'm wondering the extent to which the best
13 practices appear in your SLAs, and are used as part of
14 your SLA process with your customers.
15 MR. MAGANA: Yes, I mentioned SLAs. We're
16 pretty transparent with our customers about what our
17 SLAs are and how we derived them as far as for things
18 like time to repair. We've boiled it down to
19 different internal SLAs like time to isolate and those
20 sorts of things from a repair perspective, but the way
21 we develop them is we've done studies from loss of
22 redundancy and how many hours a loss of redundancy may
23 stand before it could create an outage and those sorts
24 of things, and we've tailored our SLAs to be candidly
25 more aggressive than what we have to report to the

1 Commission.

2 An example, SF-7 outages, I think the

3 tolerance is 30 minutes. From a Level III

4 perspective, we classify it as an outage within five

5 minutes and handle it that way, so we will always be

6 ahead of the curve. We'll still report even if it

7 doesn't match, you know, the Commission's

8 requirements. So those are the type of things we take

9 into consideration from an SLA perspective.

10 MR. KEECH: I think an SLA from our

11 customers' perspective is a financial incentive for us

12 to perform. The conversations we have with customers

13 around SLAs is they tell us, I hope you never have to

14 or I never have to invoke this as your customer. The

15 conversations we have with customers after an outage

16 or a failure of some sort are not about how soon are

17 you going to credit my account, it's what are you

18 doing to ensure it doesn't happen again, and when can

19 I expect that to be implemented.

20 And we do the same thing with our service

21 providers where we're buying capacity from somebody

22 else, for example. We hope we never have to invoke

23 them. So the SLA terms typically need to be a large

24 enough incentive so that the service provider goes

25 back into their own organization and says, okay, how

1 do I avoid, one, not meeting my customers'
2 expectations according to -- you know, as defined in
3 the SLA, and looking to the encyclopedia of beset
4 practices to make sure that we are following those to
5 the degree necessary and appropriate in order to meet
6 those requirements because the conversation, again, is
7 not about even meeting the metrics that are in there,
8 in the meantime to repair, it's, I didn't want the
9 outage to occur at all, and while you're paying me for
10 it, I'm really more interested in how you're going to
11 avoid it in the future.
12 MR. MAGANA: One is too many kind of thing.
13 MR. GOLDTHORP: So I'm wondering how
14 sophisticated customers are getting in terms of their
15 awareness and knowledge about the communications
16 industry. Do they --
17 MR. KEECH: Very sophisticated.
18 MR. GOLDTHORP: So do customers come to you
19 when they're negotiating a contract for -- negotiating
20 an SLA and say, okay, I want to prevent a --
21 MR. BUGEL: It could be negotiate on the
22 SLAs. I mean, that could be the primary driver for
23 the customer. Cost may not be the primary driver.
24 MR. MASTER: And I think part of the issue
25 is the SLAs has to be and has become a necessary

1 component of what it is the customer is buying, and
2 like Jim is saying sometimes it's the biggest
3 component of what the customer is buying.
4 The problem I think in the industry is that
5 the cost of providing the communication service is
6 relatively small compared to the financial or other
7 kinds of damage that the service requester is going to
8 experience if your communication goes down.
9 So you can choose to refund, you know, for a
10 one-hour outage one month of credit, but it doesn't do
11 economically any justice to the person who is getting
12 it. So that's why the conversation is not around, you
13 know, gee, I want more money back from you, it's like
14 how can I stop this from happening.
15 MR. GOLDTHORP: But wouldn't it be a good
16 way if you're a customer, right, and you want to
17 negotiate an SLA that gives you more confidence that
18 this event that you're describing will never happen,
19 wouldn't you insist on some -- you know, I want to
20 make sure that you're implementing these best
21 practices and that's in the SLA. Now, of course, the
22 SLA. the remedy in the SLA is going to be the remedy
23 that Maneck is describing, right. I don't know if
24 that stuff is even documented in SLAs, or is it mean
25 time to repair or is that the level that these things

1 get into?

2 MR. MAGANA: They get a lot deeper from a

3 customer perspective, and ask you're going through

4 negotiations with customers on SLAs, you know, there

5 could be different costs associated with a more

6 aggressive SLA. So if they want something that is not

7 typical, that it's not industry typical or even from a

8 competitive perspective, we'll explain what the cost

9 is to them. Costs could include another build, you

10 know. Cost could include from an SLA perspective on-

11 site spares, for example, maybe at their facility or

12 something, or something like that that's dedicated to

13 them.

14 So they can tailor SLAs based upon the

15 contract but typically from a SLA perspective that we

16 normally offer it's still pretty aggressive, and we

17 don't typically hide around averages like mean time to

18 repair. There will be many times specific language

19 about time to repair which will be measured in hours

20 and those sorts of things. So the customers are very,

21 very sophisticated from that perspective.

22 MR. KEECH: I think, too, the customers --

23 you know, the kinds of customer we offer typically

24 SLAs, they speak to the kinds of practices defined in

25 the various encyclopedia of best practices even though

1 they may not be aware, for example, of the catalog of
2 ANRAC recommendations, redundant data centers,
3 redundant egress feeds, the ability to check and
4 ensure at some point in time the fail-over-status, you
5 know. Every quarter or so let's actually run a test,
6 those kinds of things are the kinds of discussions
7 that we have with those types of customers. They ask
8 to make sure that we have those capabilities even
9 though they may not directly reference any source
10 material for them.
11 MR. GOLDTHORP: We've got about a half an
12 hour before we break, so what I thought we would do is
13 spend some time now on the third topic area, which is,
14 you know, surges in traffic and how communication
15 networks adapt to that today, so that maybe 15 minutes
16 or so on that, and then I will just open it up, you
17 know, unless we keep going on that, open it up and see
18 if the folks on the floor -- I'm not sure if we have
19 the capability to have people from online asking
20 questions, but we'll take some questions from others.
21 Okay?
22 So the third topic area like what we
23 experienced in D.C. in February and other parts of the
24 east coast, like what we anticipate, you know, if
25 there is ever a serious pandemic that causes people to

1 be needing to work from home in large numbers. I'm
2 wondering how communication providers today can apply
3 their technologies to coping with those sudden surges
4 or migrations of traffic from traditional centers of
5 capacity and traffic in sort of urban areas or where
6 Enterprise customers are clustered to more residential
7 edge networks.
8 We've talked a little bit about edge
9 networks already and how, you know, the whole network,
10 maybe they are the least able to handle capacity. So
11 how able are they to be diverse and to handle swings
12 in traffic? Anybody want to -- Jim.
13 MR. BUGEL: Network management. There are
14 multiple tools to manage search capacity and to manage
15 stranded or isolated nodes. Recent examples,
16 earthquake in Haiti, earthquake in Chile. What all
17 carriers did in the U.S. in order to make sure that
18 what existing facilities were not crushed by inbound
19 traffic is we throttled the traffic going into those
20 locations, allowing traffic to get out. That is at
21 its simplest form, but there are multiple tools that
22 we use and need the ability to use because it doesn't
23 have to be an earthquake. It could be a fiber cut in
24 a portion of a city that you have to implement these
25 techniques in order to manage the traffic.

1 MR. MAGANA: I would agree with that. In
2 the force majeure type of events, you know, you would
3 throttle the traffic and those type things. In a
4 pandemic, an example where a -- you know, a weather
5 example. The congestion might occur at the edge but
6 at the core you would be able to manage the traffic.
7 MR. MASTER: You have a lot of network
8 management capability that does a lot of things
9 internet work to facilitate whatever it is that
10 happens, and at the end of the day it is the overload
11 that's going to kill the network, not physical damage
12 or anything else by itself. Whether you have physical
13 damage or not, it's the overload that kills the
14 network, okay?
15 Now, I don't know if you've had this
16 experience and maybe, you know, the FCC doesn't have
17 this problem, but most companies appear to, which is
18 if everybody is at home and trying to work remotely,
19 it turns out that at the far end the company is unable
20 to support all these multiple users working -- trying
21 to work remotely. It's not the network that typically
22 has the problem.
23 MR. GOLDTHORP: It's the edge.
24 MR. MASTER: It's not the edge. Well, it's
25 the edge but at the other end of the edge.

1 MR. GOLDTHORP: Different edge.
2 MR. MASTER: Different edge.
3 MR. GOLDTHORP: It's not the edge you
4 expect, right.
5 MR. MASTER: And so, you know, to me it's
6 like, you know, where is the single point that seems
7 to be the most stressed, and it doesn't appear to be
8 the network, whether it's the edge network or the core
9 network in most instances. But again, I think if you
10 have some severe damage where you have multiple nodes
11 damage from, you know, whether it's a manmade or a
12 natural event, I don't think you have a choice but if
13 you don't do the right kind of network management
14 traveling and selecting traffic that goes in and out
15 correctly, you'll kill the network a lot faster than
16 anything else.
17 MR. ADAMS: I agree with everything that's
18 been said. Certainly network management is the key
19 both from either automated or manual processes to make
20 sure that you have good management capabilities to
21 swing traffic if you need to.
22 I would add on that I think the other
23 element of this is more on the human end and the
24 preparation end is making sure that you have good
25 solid business continuity plans, conduct table-top

1 exercises, right, to exercise that, and what would you
2 do in the situation, and then through various tools
3 and methods and processes make sure that things are
4 behaving the way that you expected them to behave
5 given those extreme circumstances, and I think that
6 type of planning activity is key to ensuring that you
7 can restore service if it actually does go down as
8 quickly as possible in an emergency.
9 MR. GOLDTHORP: David, do you want anything?
10 I wanted to pick up on that point that you
11 were making, Maneck, and that is, I think this is what
12 you were saying and tell me if it's not, that in a
13 typical Enterprise situation, right, the sort of the
14 conventional wisdom is that you have a bunch of people
15 working from home. They've got skinny pipes in their
16 residential access networks and they are clogging them
17 up because some of them are shared, and that causes
18 their performance to suffer, right.
19 On the other hand there is a pipe going from
20 the point of presence serving the Enterprise itself,
21 right, and then there is server capacity at the
22 Enterprise, right, for remote access, and whether the
23 pipe hasn't been provisioned with enough capacity to
24 support the traffic load in the kind of situation
25 we're describing or whether the port capacity on the

1 server isn't high enough, but to what extent are those
2 customers versus -- I mean, a customer can order a
3 large enough circuit to suit their, you know,
4 continuity of operations needs, right, whereas
5 residential access networks are provisioned based on a
6 different set of economics, right?
7 MR. MARTIN: I guess, I'm not a carrier, I
8 can say this over and over again. These were are
9 purely economic decisions, and in this particular case
10 it's --
11 MR. GOLDTHORP: Enterprise.
12 MR. MARTIN: The Enterprise has made the
13 decision that it doesn't want to order a large pipe
14 that is waiting and sitting there for that use one day
15 a year, and it isn't the network. You know, whether
16 it's support capacity under equipment, the size of,
17 you know, I ordered an OC12 instead of an OC48 which
18 is what I needed, whatever it is.
19 Now I think from a network perspective and
20 the service provider industry perspective, I suspect
21 that there are ways in which you can go ahead and
22 order, you know, with two weeks or one month or
23 whatever your carrier allows, advanced notice a bigger
24 pipe if you think there are going to be certain events
25 taking place in the next month. So you could

1 temporarily change how you deal with this stuff.
2 Again, but I think what I see is a bigger
3 Enterprise problem than a bigger network problem is
4 the way I have typically experienced it under
5 overload.
6 MR. MAGANA: It will be dependent upon the
7 customer's business continuity model, and whatever
8 they require we're happy to provide.
9 MR. GOLDTHORP: Okay. We haven't talked
10 much about events like this that have happened in the
11 recent past, and the most recent one I've described a
12 couple of times or mentioned. Do any of you observe
13 in your traffic data during events like this, do you
14 observe a spike in traffic or anything that would
15 interfere with, or does it affect your operation at
16 all or is it barely noticeable, these things that have
17 happened?
18 MR. BUGEL: Events like this?
19 MR. GOLDTHORP: Yes.
20 MR. BUGEL: Well, we monitor on our entire
21 network minute by minute, hour by hour from the
22 previous day, previous week, previous month, to
23 recognize as quickly as possible any anomalies. And
24 you do see those anomalies based on American Idol
25 voting or pick the event you see these things

1 happening. To the effect that it has any degradation
2 to the network, that's all the procedural stuff that's
3 been talked about before and that your management
4 techniques and how you deal with it. But you see it,
5 you see it, and you see things that are, quite
6 honestly, unexplainable.
7 The snow event, you know, was obviously
8 large here in D.C. but one event that we saw during
9 the inauguration of President Obama was we saw a
10 tremendous spike in UDP traffic 15 minutes before the
11 swearing in, and we didn't really know at that minute
12 what it was, but we quickly determined what it was was
13 all the multimedia stuff going over the network, both
14 wireless and wireline, and you know, I was actually
15 talking to somebody on our knock and they said, well,
16 you look at 2 million people holding up their cell
17 phones, you kind of figure out what's happening.
18 So that was, you know, you see that stuff
19 and it happens instantaneously.
20 MR. ADAMS: So again network management is
21 key. I think the key point here that keeps being
22 brought out is that it's, you know, having the right
23 tools in place to management your network and the
24 flexibility to adapt, you know, because each event is
25 different. I think testament to the network as a

1 whole, I mean, fiber cuts happen every day, there are
2 things that happen every day, the majority of which
3 never impact a customer because we do have that
4 flexibility built into our network management process.
5 I mean, the network is very reliable. Occasionally
6 we get these huge events which is really catastrophic
7 which takes more of a challenge to deal with but
8 having the right tools and a process and the right
9 business plans in place to what you would do in those
10 emergencies is key to helping ensure that we're
11 minimizing the impact of those events.
12 MR. GOLDTHORP: How is moving to broadband
13 IP-based technologies change this, made it easier,
14 harder and every way you can imagine?
15 MR. KEECH: I think from our perspective
16 it's made it easier in that to the point made, it
17 seems to be much easier to identify much more quickly
18 that a problem is occurring, and we have surveillance
19 tools that tell us immediately what, you know,
20 capacity changes that have occurred on any given link
21 in any given portion of the network. We have just
22 begun to implement technology that allows us to see
23 the type of traffic that may be flowing over those
24 lines, which gives you a much greater amount of
25 information to begin to assess the nature of the

1 problem; indeed, what it's potential root cause is and
2 you may have had in the Legacy TDM world in the past.
3 MR. GOLDTHORP: Anybody else?
4 Do you have the same capabilities that you
5 have today, the same ability to do what you want to do
6 today?
7 VOICE: I'm sorry, what was the first part
8 of your question?
9 MR. GOLDTHORP: We'll talk later.
10 MR. MARTIN: I think the ability that the
11 provider has has gone up but also the ability that the
12 user has to put more stuff of different kinds and
13 different flavors at different times somewhat
14 unexpected by you, you know, until you stop for a
15 moment and say, you know, I should have thought about
16 that, and that's sort of the lesson, I mean, if you go
17 back. I think it was the Bruce Springsteen ticket
18 even in the eighties that caused actually a network
19 failure that said no, no, no, it can't happen again,
20 and it hasn't happened again. It doesn't matter how
21 many American Idols or whatever else, inaugurations,
22 because the network understand what it is that has to
23 be done, recognizes that it's happening and does it.
24 So I think as more of these events sort of
25 happen it's like inoculation. Hopefully it will

1 happen in a small dose initially so you get to learn
2 it quickly so that when the big dose comes in you're
3 safe. That's kind of what I think is happening as
4 we're all learning together.
5 MR. GOLDTHORP: Returning now to the best
6 practices voluntary incentives theme and now talking
7 about these sorts of surges in network traffic, are
8 there areas where additional best practices or
9 voluntary incentives would be helpful to try and move
10 things to a better place?
11 MR. ADAMS: I believe continue to expand the
12 database and update the database that exist through
13 ANRAC 7 that is now keyed up. I think that would be a
14 good thing to get more people to participate, you
15 know, broaden it out, and then keep that evolution of
16 those best practices current would be a very good
17 incentive.
18 MR. GOLDTHORP: Okay.
19 MR. KEECH: I think it's always of value to
20 continuously reevaluate to say the ANRAC or ADIS or
21 someone has accomplished its task at some point in the
22 past and ignore the changes in the technology, and not
23 look at it is functionally the equivalent of putting
24 in place a network for a customer or redundancy in
25 your network and never testing it to see whether or

1 not it's working the way that you had intended it to
2 work when you first put it in place.
3 VOICE: -- process people systems. Anything
4 we can share from an experience perspective would be,
5 to your point, would be beneficial.
6 MR. MARTIN: I think the whole best
7 practices stuff that we have done has been extremely
8 valuable in the industry, but I think as the business
9 becomes -- business of corporation and business of
10 government becomes more and more increasingly
11 globalized, I think there is an assumption somehow
12 that all of us make but the global communications
13 structure which is critical to run that business is
14 somehow operating as well as it was operating before,
15 and I'm not sure that's true.
16 So that, you know, in terms of trying to get
17 some more bilateral or multilateral agreements on how
18 we do things from a communications point of view
19 across the board would probably be a very useful thing
20 for the FCC to look at.
21 MR. GOLDTHORP: Okay, one last question, and
22 then we'll go and open it up to questions from the
23 floor, and that is, in CISRIC we have a working group
24 now that's working on priority service requirements,
25 and it's intended to try and address this problem,

1 which is, we've got priority services now for
2 telephone, for plain old telephone service, for
3 wireless services, we don't have a -- although we're
4 further along on the technical side of this that on
5 the regulatory side -- we don't have a scheme like
6 that for IP-based services, and so the question for
7 CISRIC is what are the kind of requirements that
8 should be included in there, and I'm wondering if you
9 all have any suggestions, ideas, advice that you would
10 give to a group of like that that's working on a
11 service that would try and make priority access or
12 priority service available to those with the
13 particular need for it.
14 MR. MARTIN: Are you talking about the SWPS-
15 like things?
16 MR. GOLDTHORP: SWPS.
17 MR. MARTIN: Are you talking about those
18 kinds of services?
19 MR. GOLDTHORP: Yes. Yes, there is a work
20 project at NCS on this.
21 MR. MARTIN: So I think you know a little
22 bit of my background, I have sort of dabbled in that
23 for the last 25 years. I think if you look across the
24 globe, we are somewhat unique as a nation in terms of
25 having that kind of capability, which is, you know,

1 everybody has these special military networks that are
2 used for whatever, special government networks that
3 are used in times of crisis or whatever you want to
4 call them, and everybody has a public infrastructure
5 that they use for regular day-to-day use for
6 everything else.
7 What we decided to do about 50 years ago or
8 40 or whatever the number is, about 50 years ago now,
9 is to build the incremental capability on the top of
10 the public network structure for those kinds of
11 services, and if you look at the history of how it has
12 served us, I would say it served us, you know, very,
13 very well.
14 So I think from a regulatory perspective I
15 would say yes, it would be an important thing to make
16 sure that it has been moved to a new and different
17 kind of infrastructure we preserve some ability of,
18 you know, to continue to do that kid of a function
19 using the communications networks.
20 MR. GOLDTHORP: Anybody else care to comment
21 on that?
22 MR. BUGEL: I agree that we need to continue
23 to work in this area, and I think the CISRIC group is
24 a good place to start. I would encourage that in the
25 wireless environment that work continue to be done as

1 rapidly as possible. As we've talked before, we are
2 in a global marketplace, and priority mechanisms are
3 being discussed. We need to understand what the U.S.
4 Government requirements are so we can input that into
5 the process.
6 MR. MARTIN: And you're familiar with the
7 thrust of the NCS to kind of, you know, works, so we
8 work with the whole industry to get that moving.
9 MR. GOLDTHORP: So let me turn now to you
10 here in the audience, and I'm not sure if we can take
11 questions from the internet or not. Okay, so just
12 anybody in the room care to, or have a question. Sir,
13 there is a microphone right there.
14 MR. SANDRI; My name is Joe Sandri. I am an
15 SVP with FiberTower, we're a back-all provider in the
16 U.S. An observation, a congratulations and a
17 question.
18 The observation was I think Dr. Master hit
19 on the theme about there is not really a worldwide
20 standard globally for this issue that's essentially
21 been signed up by the variety of governments that
22 particulate maybe at the IEEE there is some work. I
23 do know that with the ITU processes that we've used
24 historically both on wireline and wireless management
25 for spectrum management, satellite and other areas, I

1 guess I'd suggest that the FCC spend a little bit more
2 time in developing resources with NTIA and its sister
3 state department to establish working groups in that
4 are, maybe have a new wave there because we have
5 signed treaties before, across border initiatives,
6 historic -- I mean, ITU is historically the
7 International Telegraph Union, and we've been doing
8 this since the 1880s, and hopefully that would be an
9 area to surge into. That's the observation.
10 The congratulation was that, at least to our
11 reading, the national broadband had a very specific
12 set of observations and recommendations when it came
13 to network reliability. It did embrace the post-9/11
14 section of 414 standard for diversity requirements.
15 It's Public Law 108-447, Section 414, and that was, I
16 thought, very useful to be placed in the national
17 broadband plan as a standard for network reliability
18 and resiliency, and the fact that that had also --
19 congratulate the national broadband plan in the sense
20 that that has been transferred into how that can be
21 procured nationally. The FCC basically stated the GSA
22 networks contracts spelled with an X can be used for
23 procurement now by state and local governments as well
24 for this new idea for a national public safety
25 network, so that seemed to be quite useful again to

1 our reading, and that sort of comes to a question.
2 You know, because you can't walk into this
3 building without there being two exits, any federal
4 building is uniform, any federal highway we drive on
5 is uniform, any airplane we get on that goes over
6 water has to have two engines or it's not allowed to
7 take off. So taking those standards in the national
8 broadband plan and bringing them much more
9 aggressively to the forefront for government contract
10 as well as maybe for global standard I guess, is that
11 realistic in the short term or mid term is the
12 question? Thank you.
13 MR. GOLDTHORP: Jorge, you look like
14 you're --
15 MR. MAGANA: Realistic, in the short term I
16 would say it's pretty aggressive, obviously in the
17 short term, but you know, the standardization, you
18 know, because we intermingle so much with our fellow
19 carriers and service providers, you know, there is
20 some standardization that takes place.
21 Now from a global perspective short term I
22 think that's pretty aggressive, to be candid.
23 MR. GOLDTHORP: Maneck, I know you want to
24 say something.
25 MR. MARTIN: Well, I think we touched upon

1 some of this in some of your earlier questions as
2 well. You have the ability now with, you know, large
3 fiber cables, whether they are terrestrial or
4 undersea, but this problem obviously is much more
5 acute with undersea cables, but you have the ability
6 to have a very, very large cross section of traffic
7 going through them. So if you have relatively severe
8 damage on a multiplicity of these cables, you don't
9 really have much of a recovery mechanism. It's not
10 like you're just going to, you know, send a traffic
11 wire satellite, right? Satellite capacity in the best
12 of instances is maybe a single digit percent of all
13 what was going on cables, and you're not going to just
14 start laying undersea cables all over the world just
15 so that when you have an event you will be able to use
16 them for diversity because the market doesn't really
17 want to pay for that, correct?
18 So, I don't know how some of these problems
19 can be solved except if there is some other mechanism
20 that demands that that happens and pays for it. It's
21 not the market.
22 MR. GOLDTHORP: Sir? Would you mind coming
23 to the microphone, please?
24 VOICE: Yes, I'd like to know from a
25 security perspective from the panel on what is your

1 take on migrating from IPB 4 to IPB 6, and what are
2 the security implications on that?
3 MR. MARTIN: It used to be the holy grail
4 before it became address size.
5 MR. GOLDTHORP: There must be some security
6 implication one way or the other, right? I guess so.
7 MR. MARTIN: There is an awful lot of IPB4
8 out there that will be transitioned when it's
9 economically feasible for a lot of Enterprises, so you
10 know, unlike a country where, you know, you're just
11 building an infrastructure and it's a small country
12 and you can be IPB 6 years ago; thinking about South
13 Korea and other places. So I think we are on a path
14 to get everything IPB 6, but it's not just going to
15 happen because -- I think we have made IPB 4 much more
16 secure than it used to be.
17 MR. GOLDTHORP: Anything else? Harold?
18 MR. SALTERS: Harold Salters, T Mobile.
19 Jorge, I thought it was you who mentioned an
20 encyclopedia of best practices, and I'm just curious.
21 Is the encyclopedia of best practices the ANRAC best
22 practices or are there other sets that are consulted
23 in terms of network design and management?
24 MR. MAGANA: I think Mr. Adams mentioned it,
25 but there are some. I mean, there is the IDL best

1 practices that some folks implement. There is some
2 ITU recommendations that we all look into, but I think
3 it was Mr. Adams who spoke of that.
4 MR. KEECH: I think it was me.
5 MR. MAGANA: Sorry.
6 MR. KEECH: I was referring to -- I was
7 specifically referring to ANRAC which is the ones that
8 I am most familiar with. There are undoubtedly across
9 a plethora of IT and related industries a number of
10 best practices. I was specifically referring to ANRAC
11 at that point.
12 MR. SALTERS: I guess the thought is right
13 now the CISRIC process is focused on the ANRAC best
14 practices, and I'm just thinking are there others as
15 well that could be looked at or referred to as part of
16 that process?
17 MR. ADAMS: Well, I'm on the 2B committee,
18 which is media security reliability. That has a body
19 of best practices as well. We're just getting geared
20 up on it, but the intent of that committee is to
21 actually look at the existing best practices and
22 update them, so there is definitely a lot of other
23 sets out there. Some of those are obviously included
24 in CISRIC but there may be others that are not, so
25 maybe that should be looked at.

1 MR. GOLDTHORP: Harold, let me also try to
2 answer your question. The working groups over the
3 years have gone at this in different ways. So for
4 example, the working groups in previous ANRACs that
5 worked on the cyber security best practices didn't
6 just use -- didn't just start from the ANDAC best
7 practices when they did their work. Most of their
8 work, in fact, this may be true for a lot of the best
9 practices, they were -- it was gleaned from other
10 sources, IETF, you know, ITU, other, and it's cited,
11 it's heavily cited. So we don't discourage that sort
12 of things, folks from going out that are working on
13 working groups from going out and embracing the body
14 of knowledge wherever it may be, and I know that's
15 been done in other working groups, and certain nobody
16 is stopping that as they are kind of examining the
17 best practices again now.
18 All right, any other questions this morning?
19 Sir?
20 MR. TAVARES: Good morning, I'm Tom Tavares
21 from Expirix.
22 The question I had was regarding broadband
23 initiatives and the FCC plan of kind of rolling out
24 broadband to different segments that aren't served
25 right now through normal providers. You had a

1 question, what is different now with IP or IP services
2 compared to what they were in the PSTN, kind of got an
3 answer I didn't expect because, again, from what I've
4 observed is as they go, as the service providers, and
5 not just the ones here but, for example, as they go to
6 IP these things just don't stand up under certain
7 cases that you -- you mentioned American Idol storm --
8 where a government entity is sending out thousands of
9 calls to warn people in other instances, and you have
10 things where soft switches are being overloaded or
11 gateways or things like that, and again just starting
12 from Cox down, what metric do you look at to get an
13 early warning system in these new broadband services
14 and again avoid being the canary in the coal mine?
15 When I look at my old broadband router, I
16 can always see, okay, the voice is down, and then I
17 see the other multimedia applications. What do you do
18 as far as, you know, managing your network, monitoring
19 your network? What basic metric do you look at when
20 you know something is wrong? And I guess that's for
21 everyone.
22 MR. MAGANA: Well, I don't know the specific
23 names of the systems but I can get them, but overall,
24 I mean, we look at a lot of our capacity type
25 management utilization, circuit utilization both on an

1 automatic and on a manual basis, and then we basically
2 review that and if there is areas of saturation or
3 more saturation than we expect, then we take action
4 through network management process to mitigate those
5 highly utilized circuits, so there is both automated
6 and manual processes involved in monitoring and making
7 sure that we're keeping our network optimized.
8 MR. TAVARES: A follow-up question to that
9 is in the old TVM world you kind of looked at, you
10 know, circuits, and now we look at pipes, but it's
11 more than just looking at the health of the pipe. You
12 have to look at, you know, how is the end user being
13 affected. Do you drill down to the end user or do you
14 still look at pipes or what do you see?
15 MR. MAGANA: We've had wipe technology for
16 years that we've been providing service on. Yes,
17 there is definitely the network layer, but we also
18 have, you know, same type of capabilities that we
19 would on the wireline from a switch perspective. We
20 look at both call drops, call completions, quality of
21 service type metric through various network management
22 tools that we have. So we are monitoring it from a
23 network perspective but we also do monitor from an end
24 user perspective.
25 MR. TAVARES: Okay, thank you.

1 MR. BUGEL: From AT&T's perspective as I
2 said before, we're monitoring the global network and
3 we break that down into different modalities and
4 different regions. Simultaneously we're working
5 anywhere from about 150 to almost 200,000 potential
6 cyber cases during the course for the 24-hour period.
7 Not all may turn out to be cyber cases, but there may
8 be as many as 30 or 40 escalate to that point. We're
9 also monitoring multiple Bot nets and Bot net masters
10 around the world. All this is happening
11 simultaneously, so if we see an anomaly in the
12 traffic, and then we also have the network knowledge
13 that there's a fiber cut or something like that, we
14 also see what's going on.
15 So all that stuff is being monitored and
16 basically what we're looking for is we're looking for
17 that slightest degradation in your service, and so any
18 anomalies that go through, then we start taking
19 network -- we take network management techniques to
20 improve that or bypass that, and all that stuff is
21 happening simultaneously so there is a lot of things
22 that are being looked at on a minute-by-minute basis.
23 MR. TAVARES: Just a last follow-up
24 question. Do you monitor just your networks or do you
25 monitor all your pairing partners because again with

1 an emergency service you're going to have to go across
2 different carriers to complete that call?
3 MR. BUGEL: We monitor our networks. We
4 also are in constant contact with our pairing
5 partners. I will tell you that what transverses our
6 network, we know 99 percent of the traffic where it
7 comes from and where it's going to and who it came
8 from, so we're very familiar with all the traffic, and
9 we have the ability to communicate to those people.
10 MR. TAVARES: Thank you very much.
11 MR. GOLDTHORP: Well, thank you all for
12 being here and joining me. I want to thank our
13 panelists today.
14 (Applause.)
15 MR. GOLDTHORP: And we'll be starting our
16 second panel at 10:45 so that gives everybody 15
17 minutes to freshen up.
18 (Whereupon, a short recess was taken.)
19 MR. GOLDTHORP: The second panel this
20 morning deals with the matter that Jamie started to
21 talk about in his opening remarks, and that is the
22 Commission now has a data collection regime on the
23 books where we are getting information about
24 communications on Legacy networks and Legacy
25 technologies, and this information, while it hasn't

1 been particularly helpful to us say in identifying
2 cyber intrusions and the like, is very, very helpful
3 to us in knowing where there are reliability issues in
4 the network that aren't only evident but statistically
5 significant, so we don't tend to use this data for one
6 off things, we're using it to measure trends over
7 time, and then we work with industry either
8 individually or we work with carries through industry
9 forums like ADIS and NRSC, and then we can measure
10 what happens after that, so it turns out to be very
11 helpful to us.
12 We don't get any data right now on ISPs or
13 broadband ISPs, so we don't have the benefit of that
14 awareness or that kind of a program for continuous
15 improvement, and the question now has come up or a
16 recommendation has been made in the national broadband
17 plan that we should go about getting that, and
18 questions are what should we be collecting assuming we
19 were to go forward with this? How should we do it?
20 Should it be under the same kinds of regulatory
21 framework as the way we did it in Part 4 in the rules
22 that we have on the books now? That's a question.
23 So I want to touch on all of those in turn
24 today, but before I get started with that let me ask
25 our panelists to introduce themselves just as we did

1 in the first panel, just a few remarks very briefly,
2 and we're going to start with Jim and work our way
3 back up this way this time.
4 MR. BUGEL: Good morning, I'm Jim Bugel with
5 AT&T. I'm assistant vice president of public safety
6 and homeland security. Encompassed in that is cyber
7 security, network reliability and emergency
8 preparedness.
9 MR. WOUNDY: Hi, I'm Rich Woundy from
10 Comcast Cable. I'm SVP of software applications in
11 our CTO office, so I'm looking at future capabilities,
12 but I'm also one of the people that was working on
13 congestion management and how applications react to
14 congestion on broadband internet.
15 MR. KEECH: My name is David Keech. I'm
16 assistant vice president of engineering with Frontier
17 Communications. I currently have responsibility for
18 day-to-day operations of our internet service provider
19 organization and prior to that I was also responsible
20 for the management of our knocks on a day-to-day
21 basis.
22 MS. BOOTHBY: I'm Colleen Boothby from
23 Levine, Blaszak, Block & Boothby. I'm the odd woman
24 out on the panel. I'm not an engineer, I'm a lawyer
25 and I represent not carriers but Enterprise customers

1 who are concerned about these issues because the more
2 data they can get as their networks become 100 percent
3 IP the better, and while they applaud the broadband
4 plan's recommendation to start collecting some of this
5 data, we are concerned that the Commission's authority
6 to do that, especially after the Comcast decision, may
7 be compromised and that the Commission should think
8 about moving to a Title II basis for collecting some
9 of this information.
10 MR. GOLDTHORP: Okay, thank you, and thank
11 you all for being here today. Appreciate you joining
12 us and looking forward to digging into this topic so
13 we can get some issues or questions or data on the
14 record that's going to help us think through it.
15 Let me start by just framing it out a little
16 bit. There is two topic areas that I thought in
17 general we'd like to get into. One is what should we
18 be measuring. Assuming we're going to measure
19 anything, what should it be? What should we measure?
20 How do we know, or how would a communications
21 provider know that there would be anything worth
22 telling us about, or that would be worth our while to
23 get? And you know, starting even further back, what
24 are the kinds of failure modes that happen in IP-based
25 networks that are unique or different from what occurs

1 in Legacy communications networks?

2 The kind of failure modes that we get today,

3 for example, are -- you know, we'll get signaling

4 network outages, SS7 outages, transport network

5 outages, DS3 outages and things of that sort. But

6 what's different about IP and ISP networks -- not just

7 IP networks but ISP networks -- that should cause us

8 to be thinking about what we would be measuring

9 differently.

10 And then the second category, the second

11 topic area is how shall we be measuring it? We've got

12 a system right now called NORS that is an online

13 system that we use to collect this kind of

14 information, and we've got processes associated with

15 that communications providers do. How shall we be

16 doing that in the future? Should we do it the same

17 way? Should we be doing it differently? And we want

18 to test out or get ideas from the panel about that

19 topic as well and others as they come up.

20 But let's start with this question of how do

21 ISP and IP-based networks differ fundamentally from

22 Legacy networks that we measure today and in ways that

23 would cause us to look at different types of reporting

24 categories or criteria. Anybody want to start with

25 that? Jim?

1 MR. BUGEL: Yes. Well, basically the
2 circuit switch network in terms of outages is a hard
3 down type of network. It's an all or nothing,
4 speaking of a specific route. That's how NORS was
5 designed in a circuit switch environment.
6 The ISP networks are survivable technology.
7 The traffic will find a way to get to its
8 destination. There may or may not be degradation,
9 noticeable degradation, but that's basically the
10 fundamental difference between the two technologies,
11 and certainly to your point, there needs to be a
12 careful analysis and careful consideration as to how
13 you would even measure that amount of degradation or
14 is the degradation really not the issue and more of a
15 regional outage or regional impact the way to look at
16 it.
17 MR. GOLDTHORP: Rich?'
18 MR. WOUNDY: There is a bunch of things I
19 could talk about here. One is in terms of specific
20 failure modes that are more specific to the internet,
21 one is certainly congestion, and so in terms of
22 congestion you may see reduced bandwidth. You may see
23 higher latency or delay in the traffic. You may see
24 jitter. Jitter not so much. Theoretically you could
25 se it, but it's much more likely you're going to

1 either see less bandwidth or higher delay.

2 You can also see, as opposed to binary

3 on/off types of outages, you could see all kinds of

4 different partial outages. So you may see that the

5 whole internet is available but maybe not YouTube. It

6 may be that YouTube is available because -- just to

7 show you how screwy the internet can be, it could be

8 that somebody in China or somebody in Pakistan has

9 injected some routes into the network, and it's now

10 drawing traffic that should have been doing to YouTube

11 to Pakistan or to China and then it's getting dropped

12 by some firewall there. So that is something you

13 don't see in the TDM network.

14 You can also see different adaptations to

15 what's happening in a network too which makes it even

16 harder to measure. So a really good example would be

17 skype. So skype provide voice service and they have

18 their own proprietary kodex -- well, one is called

19 silk. It's constantly measuring what's going on in

20 the network and seeing that there is less bandwidth or

21 more bandwidth and increasing or decreasing the amount

22 of bandwidth, and very similar networks for Netflex.

23 When Netflex downloads videos, it might send it down

24 to you in HD but it might send it down to you in a

25 much lower bandwidth because it sees what's going on

1 in the network.

2 So the applications are doing things. The

3 network is doing things and sometimes other parts of

4 the internet and sometimes it's even where you're

5 going to in a network changes. That's why we have

6 content delivery networks, because they're constantly

7 moving around traffic to work around all these --

8 mostly avoiding congestion, sometimes -- once in

9 awhile creating congestion but for the most part

10 trying to work around all these things, so there is a

11 lot of active components in the internet, and I think

12 that's what makes it worth taking your time to figure

13 out how -- you know, where to pin down what's wrong

14 with some part of the internet at one point in time.

15 MR. KEECH: I'd simply add to that that, and

16 we talked earlier in the prior session between the

17 distinctions between the core and the aggregation

18 network, and I think when you're talking about

19 measuring network performance you need to take into

20 account the differences in the data that can be

21 collected in those various components of the network,

22 specifically, you know, latency, jitter across the

23 core, bandwidth utilization are fairly easy to collect

24 because you've got, you know, router switches, et

25 cetera, at those pairing points, at those points all

1 the way down into the regional aggregation networks.
2 Beyond that for regional or localized
3 aggregation network you may not have the capability as
4 it exists today to get as close to the customer as you
5 would like to be able to tell what the actual customer
6 impact is, i.e., what is the change in latency, how
7 bad is it, what is the actual end user experience
8 because conceptually at least in order to do that
9 you've got to check that experience between two end
10 points; one of which might be a point in the core but
11 the other one is, you know, to get the true customer
12 experience needs to be as close to the customer as you
13 can possibly get.
14 Practically that doesn't mean checking every
15 individual high-speed user's modem as an example. You
16 want to at least practically I think move it someplace
17 up into the network. Whether or not that's a local
18 aggregation router or an optical switch or something,
19 I think is something that needs to be looked at
20 because there is obviously a cost and a time frame to
21 implement technologies to be able to do that.
22 MS. BOOTHBY: From an Enterprise customer's
23 perspective I think a lot of the discussion has been
24 mass media or mass market customers. From an
25 Enterprise customer perspective I think we would like

1 to see the Commission collect data that tracks the
2 SLAs that we negotiate. Even though the data
3 available to the Commission is not available to
4 Enterprise customers on a service provider basis, we
5 see some utility to having data that translates into
6 the SLAs even on an industrywide basis that translates
7 into the SLA measures that are most common in
8 contracts partly because SLA is negotiated by
9 Enterprise customers are very difficult to enforce.
10 I think the earlier panel mentioned that
11 somewhat, and that as sophisticated as my clients may
12 be on engineering matters for purposes of specifying
13 SLAs without a competitive market they don't have a
14 lot of negotiated terms and conditions that allow them
15 to enforce those SLAs. So having an industrywide pool
16 of data can be very useful for them in gauging their
17 own.
18 MR. GOLDTHORP: There was a bunch of points
19 brought up but I want to go back to the idea of -- you
20 know, Rich, it was you that mentioned it, and that is
21 that you can have situations where essentially router
22 tables are, if not poison, at least have basically bad
23 routes injected into the router table, right, and I'm
24 wondering -- when you said that it caused me to draw
25 the analogy, since we were talking sort of about next

1 generation versus Legacy, to translation tables in
2 Legacy systems.
3 Now, obviously translation tables are
4 provisions, right, and whereas these are dynamic. You
5 know, BGP is a dynamic protocol, and router tables are
6 updated dynamically. So how would you measure
7 something, and what maybe amount to a cyber intrusion
8 or attack or some other, you know, disruption to
9 communications, how would you measure something like
10 that?
11 I mean, I know when translation tables go
12 down because 9-1-1 calls are going to the wrong P
13 set.'
14 MR. WOUNDY: I mean, I think what ends up
15 happening as a practical matter is end users
16 discovering this, like how come YouTube has stopped
17 working for me to take a specific example, and that
18 usually causes someone to say, well, let me see what's
19 going on, where is that traffic being routed, and let
20 me compare it against the routing tables that I have.
21 So at some point you have to say, well, what
22 is the -- what's the source of truth for those
23 particular routing cables? And that's one area in
24 which there has been much discussion and debate in the
25 network operator side because there are supposed to be

1 some authoritative tables. The regional internet
2 registries are supposed to be collecting these
3 databases in which they say there is an ISP, they have
4 a particular kind of a system, and here is all the
5 different networks that are supposed to be associated
6 with them. And in theory you could check what is in
7 your routing table versus what's in one of these
8 routing information databases, and compare the two to
9 see.
10 In fact, I think there was one attempt by an
11 ISP probably about 15 years ago to actively manage
12 that, but it's not in any core routers today, and the
13 technology didn't scale because back in those days
14 there were 10 times less routes in the route table
15 than there are today. But at least there is a
16 database that exists, and at least there is -- one can
17 do comparisons between what's in the route table and
18 what's in these different databases.
19 By the way, sometimes these databases aren't
20 totally accurate like, you know, this company --
21 company A acquires company B and now it's not accurate
22 anymore, or somebody handed back address space and
23 they forgot to inform this particular database. But
24 that's one place to start.
25 Now, there is actually something related to

1 this. There is something called looking glasses which
2 is something that I can't imagine exists in the TDM
3 world or translation tables, but it exists in the
4 internet world. You can actually get a view into what
5 the global routing tables look like in one of these
6 looking glass tables. So even the FCC, if it had
7 permission, could go to one of these looking glasses
8 and say, show me what the global route table looks
9 like for some portion of the internet, and even the
10 FCC could see, oh, look, you know YouTube there is
11 some route that's been rejected, that doesn't belong
12 here.
13 So on one sense it's a lot more difficult to
14 figure out the metric for that, but on the other hand
15 there is more and more public data information sources
16 that the FCC could tap into or other third parties to
17 say, well, what is going on, and to be able to collect
18 information without adding any new processes, which is
19 interesting.
20 So I don't know if I directly answered your
21 questions. It's kind of hard to say how to quantify,
22 you know, how often YouTube goes off line. I mean,
23 for that particular example I'm giving it, maybe it's
24 like once every three years, but when it happens there
25 is immediate attention and that's usually when there

1 is calls between different network operation centers,
2 how did this route get there, how come you're sending
3 me this route, you know, why are you saying my YouTube
4 traffic off to Pakistan. That doesn't make any sense
5 to me. I think it's handled that way. On an
6 emergency basis it's handled a knock to knock thing.
7 MR. GOLDTHORP: Okay, maybe if we have time
8 we'll come back to that because I actually have some
9 questions about that, but we talked earlier about the
10 idea that in ISP networks outages tend to manifest
11 themselves more as performance degradation, not as
12 hard down failures, and I wanted to just probe on that
13 for a second.
14 It seems to me, and tell me if I'm wrong,
15 that the closer you are to the edge the more likely
16 that an outage in that part of the network will be
17 manifest to the customer as a hard down outage. If
18 you've got a DNS outage where both DNS, you know,
19 customer had no access to DNS, that's basically hard
20 down for at least web traffic anyway, right? Probably
21 other applications of the internet as well.
22 DHCP outage for new, somebody coming on to
23 get authenticated for a network, that would be
24 perceived by the user as a hard -- denial of service
25 outage, right, they would not have access to the

1 service.

2 So those kind of outages would seem to be a

3 little bit closer to the user. DNS, maybe not so much.

4 That might be deeper.

5 The stuff that would be more performance-

6 based would seem to be deeper than the network. Is

7 that a false assumption or is there truth in that?'

8 MR. WOUNDY: It's actually kind of funny

9 because at one point we had our DNS infrastructure

10 largely centralized in our company, two locations, so

11 we had geographic redundancy, but largely cluster.

12 When we ran into some performance issues, we found

13 that the best way to resolve it, to reduce the failure

14 point as well as to provide more capability was

15 actually to push the DNS out further into the network.

16 As a matter of fact, our DNS has been much

17 more reliable and much more performance since we've

18 done that, and that was just in the last five years.

19 MR. GOLDTHORP: Since you pushed it out

20 towards the edge?

21 MR. ADAMS: When we pushed it out towards

22 the edge. So I wouldn't -- and I think for things

23 like DHP and DNS, I mean, I know that we have all

24 kinds of redundancy schemes in terms of multiple

25 servers, multiple locations and such like that. I

1 think if we're talking -- I think the one place where
2 you start to run into single points of failure on a
3 network would be as you get out to the CMTS, and we
4 try to -- you know, that's our edge router. That's
5 directly attached to our DOXES network.
6 Now, if that goes down, and that's why it's
7 usually wired up to be, you know, redundant power
8 supplies, redundant processor blades, redundant
9 network interface cards, et cetera, but if there is
10 anyplace where -- you know, that's at the edge and
11 that tends to be where you could potentially get into
12 as close to a single point failure as you are going to
13 get.
14 As you get deeper into the network you tend
15 to have more and more reliability, more and more
16 backup links, more and more multi-site redundancy for
17 different products and services. And I think like in
18 terms of congestion effects, I know I've expressed
19 this to various ITF groups, and I seem to hear very
20 similar from other network operators, you're going to
21 tend to see congestion in the last mile first. The
22 next place you're more likely to see congestion is on
23 interconnects between providers, and then the last
24 place would be in the core in terms of ordering of
25 where congestion usually happens.

1 And usually on the core it's almost -- it's
2 very rare whereas if you get out to the edge, and
3 particularly if you're dealing with my personal
4 connection to the network, obviously if I have a 384
5 kilohertz per second upstream, then, you know, self-
6 congestion is extremely likely. All I have to do is
7 upload some photos and I've congested myself, right.
8 You know, after that comes shared congestion where
9 there is a whole bunch of users that are using enough
10 capacity that they start to impact each other, then
11 it's off to the interconnects and then it's down to
12 the backbone. I hope I answered.
13 MR. KEECH: I think the commentary brings up
14 a point in terms of being thoughtful about what it is
15 you're actually collecting. Frontier's DNS
16 infrastructure is highly distributed as well in
17 multiple server forms, and during the assignment of an
18 IP address the DNS registration is given to them on
19 geographically dispersed server, so there is a primary
20 and a secondary.
21 You know, I could lose the primary and the
22 customer is unlikely to see any impact at all because
23 I've got a secondary that it immediately defaults over
24 to. I could lose two out of three servers in a DNS
25 round robin farm and there would be no impact to the

1 customer at all. Is that a reportable event?
2 I've got one or two-thirds of my
3 infrastructure down and yet there is absolutely no
4 impact on the customer either because of time of day,
5 front load, what have you. Potentially there could be
6 an impact. How do you measure that? And I think it
7 gets back to, you know, the question on the table.
8 What is meaningful in terms of the customer experience
9 versus what is meaningful in terms of an
10 infrastructure in a technology base that has been
11 designed to be redundant, and pursuant to use of best
12 practices a service provider is incented to actually
13 perform against?
14 MS. BOOTHBY: I agree. You know, the beauty
15 of IP networks is it's certainly more robust than
16 Legacy networks. I'm remembering the time that AT&T,
17 the IXC, don't worry, took down New England and Logan
18 Airport, and fixed the problem by shoving a broom
19 handle into a circuit breaker that had blown when
20 nobody was around to see it. So, yes, we've come a
21 long way.
22 From the Enterprise customer perspective, I
23 think hard down is not the issue so much as the
24 performance measures, and that's why there is things
25 written in terms of latency, jitter, and the sort of

1 performance-based measures that carriers see with each
2 other. A credit card validation network, a bank ATM
3 network has performance issues, and it's not just a
4 complete failure of the network that can be a problem
5 for them. It's the performance dropping off. No one
6 expects five nines, but still the performance dropping
7 off to impair the kind of data exchanges that are
8 critical to those.
9 MR. GOLDTHORP: That brings up a point which
10 is more of a threshold type of question, and so what
11 is the right threshold when we're dealing primarily
12 with these sorts of performance degradation problems
13 that exhibit themselves that way?
14 One way to describe it is to say generally
15 available connectivity, right, or general useful, not
16 available, it's probably general useful. So that is
17 something I struggle with because it's so subjective
18 and I'm wondering if maybe in your experience with
19 SLAs, I mean, maybe in the kinds of work that you all
20 have done you've been able to pin that down a little
21 bit better into metric that are meaningful and
22 thresholds that are meaningful in terms of what you
23 look at.
24 MR. KEECH: Well, I think certainly Frontier
25 has metric within its surveillance systems which when

1 they are exceeded cause us to begin to look at an
2 issue to determine whether or not it's creating an
3 issue. That might be capacity threshold on a circuit.
4 If we exceed it, then that alarm is going to up right
5 up on our board and somebody is going to be assigned
6 to go look at that.
7 We have jitter latency type measurements
8 across the network in certain applications where,
9 again, if they fail to meet a threshold, might be
10 under a certain threshold or exceed a certain
11 threshold, depending upon which is good or bad, that
12 will come up on the Knox board, and somebody will be
13 dispatched or targeted to look at that.
14 That varies by application, for example, and
15 doesn't always necessarily mean that there is a
16 problem. In particular, you can have momentary spikes
17 due to large downloads from Bit Torrent or YouTube in
18 a given area. That will come up on the board and will
19 disappear almost as quickly.
20 Is that an outage condition? Probably not
21 for the majority of users. For the person who might
22 have been trying to download 100 meg. file, you know,
23 they may see that whether there are an Enterprise user
24 or a home user somewhat differently. So you've got
25 this dichotomy I think of what performance means at

1 the network level and what performance means at any
2 given instant to an individual trying to use that
3 network. The network itself may not have a problem as
4 reportably by our metric. An individual who is
5 downloading a lot of large files may in fact impact
6 other users in that immediate area who have a
7 momentary problem, but when they go back to check it
8 five seconds later, 10 seconds later, that problem has
9 been ameliorated. So what's reportable at that?
10 MR. ADAMS: So just to jump off on that,
11 within our network we have tools to figure out like
12 between this router and that router, or this component
13 and that component; you know, what's the delay, what's
14 the jitter and all that. And at the edge of the
15 network we know what percentage of capacity has been
16 used.
17 So if you look over at the DOXES network
18 site, we can say, oh, look, I'm upstream, or on this
19 downstream network we're using 50 percent of the
20 upstream right now is being used, and 20 percent of
21 the downstream. But those metric are kind of leading
22 indicators as opposed to what's really happening from
23 a customer experience point of view, which we have
24 been reminded many times by the folks that are on the
25 other side of the aisle with respect to net

1 neutrality.

2 They make a, and in some ways they are

3 right, we use those as indicators. We say, okay,

4 well, if this particular DOXES upstream port is being

5 used at 90 percent of its total capacity, hmmmm, there

6 probably could be some performance issues there, but

7 the only way you could really tell is to do end to

8 end, end to end measurements such as there is all

9 kinds of internet speed tests that are out there.

10 They tend to measure upstream bandwidth, downstream

11 bandwidth, and latency to a particular point in a

12 network.

13 And what's really interesting is some stuff

14 the FCC has already started doing, as of Friday, they

15 are working with a company called Sam Knows, where you

16 take this appliance, which is essentially a Cisco

17 router that has some code on it that you install in a

18 customer's house on their broadband connection, and

19 then it will go off and do all kinds of difference

20 performance measurements.

21 So it will measure speed and latency, we'll

22 say; how long does it take to get to the DNS servers,

23 you know, DNS server is up; go off to some popular

24 websites, how long does it take to download those; and

25 so it might be really interesting to incorporate that

1 into some of the analysis because I guess the FCC is
2 already doing that from the purposes of transparency
3 from the open internet perspective, and you know, are
4 people really getting the broadband speeds they are
5 supposed to be getting from the national broadband
6 plan perspective. And it might be good to draw all of
7 that experience into this as well.
8 MR. BUGEL: I just wanted to also emphasize
9 a point about application. Is application specific?
10 Where we do have customers that have designed private
11 networks, Enterprise networks to do robotic surgery as
12 opposed to mass processing, and those we monitor, all
13 the companies monitor those applications to make sure
14 they are hitting the service level agreements, and
15 make appropriate modifications using the network
16 management tools we have capable to make the
17 appropriate adjustments to make sure that those
18 throughputs are achieved.
19 Again, I just want to reemphasize this, we
20 talked about this on the first panel, is that we're
21 monitoring the network on a minute-by-minute basis and
22 looking for those anomalies at a macro level and a
23 micro level.
24 MR. GOLDTHORP: So the way I sort of imagine
25 NORS working now though I'm sure it doesn't work quite

1 this way because when we developed the data model for
2 NORS we didn't do it with the kind of intimate sort of
3 collaboration say like we did with the disaster
4 information reporting system. That was a much more
5 sort of open process where we sat down and we said,
6 what are you seeing during a disaster, what is easy
7 for you to provide to us, what do we need, and we met
8 in the middle there.
9 Is there a way, as you think about the kind
10 of data that you collect and analyze now, is there a
11 way to start from whatever the next generation
12 version, let's say for example a NMA is, whatever kind
13 of macro management systems or monitoring systems that
14 you're using now or for next generation technologies,
15 to imagine a way to aggregate that data up in a manner
16 that would result in a useful reporting scheme? Can
17 you imagine that?
18 MS. BOOTHBY: I think the first step for the
19 Commission, I mentioned this in my opening remarks,
20 it's got to develop the authority to collect that
21 data, and there may be some significant rethinking the
22 Commission is going to have to do in the wake of the
23 Comcast decision regarding how -- where does it go for
24 the authority to collect information at the internet
25 access level of service.

1 So I think the first step is the Commission
2 has got to think through what kind of authority it has
3 to get involved in these issues from the get go.'
4 MR. WOUNDY: Well, I think what might be
5 different in this case is there may be some
6 information repositories the FCC can already leverage
7 to get at least some of this information, and to at
8 least figure out what information is needed above that
9 to make sense.
10 So, for example, Arbor Networks is a
11 company, we talked about them, they produce these
12 products, these network management products that go
13 off and collect information that says, you know, this
14 is the kind of traffic that's flowing over your
15 network at any particular point in time. What they've
16 done is then they've created this other infrastructure
17 called ATLAS that actually collects all that kind of
18 information from the remote nodes, from all these ISPs
19 that participate in this, and so they're feeding back
20 -- we, ISPs, are feeding back information such as here
21 is what's happening from a routing point of view, here
22 is what's happening from a -- you know, here are the
23 top threats that are being collected, and even a
24 certain amount of like how much traffic is flowing
25 over these networks.

1 One of the things that surprised us was
2 ATLAS started producing these reports that said how
3 big, different ISP backbones were and how much traffic
4 they were carrying because we were surprised to find
5 that we weren't in the 2007 list and all of a sudden
6 in 2009 we were like number six, and we were trying to
7 figure out how that happened, and we kind of know why,
8 because we built a backbone that helps.
9 But it was amazing that they were collecting
10 that level of information with very little effort on
11 the part of the ISPs.
12 So I think that that certainly helps grease
13 the skids for the FCC being able to collect the kind
14 of information it wants, I mean, when it's -- you
15 know, there is some kind of reporting thing, and there
16 is some kind of timeframe, you know, then we have to
17 figure out how we're going to staff that and all. But
18 if it's, you know, devices that are taking information
19 that we're comfortable in sharing and it's
20 automatically sharing that with, you know, some
21 information repository that the FCC can tap into, I
22 mean, that certainly makes things a lot easier from
23 our perspective.
24 MR. BUGEL: If there is the sensing that's
25 out there, that makes a lot of sense as he was saying,

1 as Rich was saying. I think the NORS, you know, NORS
2 is a different -- it's a different animal, and NORS
3 was built on an on or off type of environment, how
4 many customers it affected, will we find it over the
5 years with the Commission's help, but you know, there
6 is a concern about the burden and understanding what
7 the relevance is with the burden.
8 This is not an on or off situation. This is
9 a level of service that is either agreed to in a
10 contract and determined by the performance, and so
11 these are -- I think that is one way to gather the
12 stuff, the monitoring that's being done on the public
13 networks.
14 MR. KEECH: I would just add subject to
15 whatever regulatory or legal environment is relative
16 to the collection of the data, there is -- you know,
17 we've been talking about hard down or not. There
18 actually is a corollary to the TDM network. There are
19 situations where customers are hard down, right. A D-
20 slam goes off line because there is a single-threaded
21 facility failure, there is an electronics failure in
22 the D-slam itself.
23 If you're looking for a place to start, it
24 seems to me a logical place to start is you're down or
25 you're not down. Those situations are pretty clear

1 cut. I think the problem with that approach, however,
2 is that the level of aggregation with respect to the
3 Legacy TDM network has been pushed, with respect to
4 IP, considerably further down into the network where
5 you may have a D-slam that has eight or 16 or 24
6 customers on it. You may also have some that have
7 several thousand on them, comparable to a remote dial
8 tone switch.
9 But to Jim's point about to be expected to
10 report on a D-slam that has 96 customers out for 40
11 minutes because of a facility failure, Frontier alone
12 has literally approaching 10,000 different remote
13 terminals of that nature. The burden there relative
14 to the value of the information would have to be
15 questioned.
16 That said, there are situations where you
17 have -- the aggregation router itself is off line,
18 that aggregation router typically may not be
19 duplicated as it is, you know, redundant configuration
20 as it is in the core. That might be an appropriate
21 level at which to start reporting if in fact that's
22 the requirement, but I think you've got to take a
23 serious look at granularity with which or which which
24 value granularity would bring to that reporting
25 process given that the quantity of customers in those

1 remote terminals tend to be considerably less than it
2 would be in a comparable remote dial tone terminal.
3 MR. GOLDTHORP: Okay. Let's follow up for
4 just a second on this point about probes, I guess I'll
5 call them probes, right, in the communications, in the
6 IP-based or IFP internet networks, right, and this is
7 something a little -- this is something new. I mean,
8 we didn't have this kind of technology deployed by
9 third parties that was deployed in Legacy TDM
10 networks. I mean, the only source of data on those
11 networks was the service providers themselves. They
12 knew and nobody else.
13 Now we have these third party data
14 aggragators, Arbor is one, there are others that can
15 on their own just deploy measuring devices in the
16 network to collect information, and I've tended to
17 think of these as devices that are out there to learn
18 about malicious traffic in the network. Maybe that's
19 just one thing they're looking at. Maybe they are
20 also looking at performance and outage information, to
21 the extent that the outages are leading to performance
22 degradations. But I'm wondering to what extent are
23 they a surrogate for data like this coming from the
24 providers themselves.
25 MR. WOUNDY: Well, I mean, if you have

1 probes in the home, obviously the one blocking factor
2 is how many homes do you have probes in. I think
3 that's more a matter of -- a matter of time and maybe
4 a little bit of money. I mean, my understanding is
5 that these probes are -- I mean, if they are built
6 into, whether it's a Cisco home router or any
7 competitor's home router, I mean, I think the cost
8 point could get -- certainly under $100, I think we're
9 targeting less than that. I'm not sure how much the
10 FCC is targeting for its Sam Knows trial.
11 But I can even imagine that if you can look
12 out three to five years you can start to build in that
13 kind of functionality, that kind of probe
14 functionality into standard home Gateways, and then
15 when customers buy it off the shelf, they can all be
16 reporters if they wanted to, and then it's just a
17 matter of building the back end infrastructure.
18 But, I mean, yeah, the internet really does
19 sort of change the game here. So as many of those
20 probes you can get out there, as long as they're not
21 all turning into a denial of service and attacking our
22 network would probably be just fine. You know,
23 certainly if there were 50 of them that all decided to
24 test the maximum amount of bandwidth at the same time,
25 that's probably not desirable, but I think there is

1 technical ways we can work around that.

2 In terms of finding cyber security issues in

3 our network, I'm not sure the right place to have the

4 probe is in the home. There is a lot of those

5 devices, even including home Gateways, that can be

6 subverted and taken over. So usually that kind of

7 probe would be more in our regional access network or

8 some aggregate -- you know, near where the aggregation

9 router would be.

10 And there is all kinds of different

11 technologies there, everything from light touch,

12 something like NetFlow to D-Pack inspection, which

13 comes with its own issues. Certainly privacy being

14 one of the biggest ones. But I mean, that would be

15 another way to collect information.

16 I think Arbor uses NetFlow information but I

17 think they use other bits of information as well, and

18 they have a very interesting webpage where they'll

19 show all the top threats that are going on right now

20 across the globe, you know, which countries are

21 attacking more than other countries, and so it's

22 amazing how much third party intelligence can be

23 gathered from the internet.

24 MR. GOLDTHORP: Colleen, you were asking or

25 mentioning earlier that the situation for Enterprise

1 customers, or at least as they observe it, is a lot
2 different than how it's observed by a residential
3 customer, the mass market customer. So would you
4 recommend or suggest that the Commission would care
5 about would be different for Enterprise customers?
6 Does it require a whole different look at what we
7 would be asking for?
8 MS. BOOTHBY: Well, it is a different
9 market. There are existing measures, things that need
10 time to repair, that kind of thing, there is a whole
11 tradition of metric in the SLAs that customers
12 negotiate. In many respects the enterprise market can
13 be much less competitive than the residential if you
14 consider that a lot of residential customers can
15 choose from cable-based or telco-based service, or
16 wireless service, and Enterprise customers tend to
17 have fewer suppliers to choose from.
18 MR. GOLDTHORP: How did you bring up whether
19 or not they are selection providers?
20 MS. BOOTHBY: Outage reporting?
21 MR. GOLDTHORP: Yes, how would that help?
22 MS. BOOTHBY: Outage reporting like your
23 MPLS network isn't as reliable as Verizon's?
24 MR. GOLDTHORP: How would that help
25 additional providers being available to them?

1 MS. BOOTHBY: Oh, well, the competitive
2 issue is that the SLAs become less meaningful when a
3 market is less competitive because in order to police
4 them you don't just pick up your network and go.
5 Because the market is less competitive, Enterprise
6 customers cannot extract contract terms that create
7 financial penalties for violations of the SLAs. The
8 major providers use the same approach that they have
9 used for years in their tariffs, which is that a
10 violation of an SLA allows you to get a refund of the
11 charges for the time period that the service wasn't
12 available, but no consequential damages, meaning no
13 recovery of the damages that the Enterprise customer
14 suffers as a result of the outage.
15 So with the lack of competition means that
16 no matter how sophisticated you are a customer cannot
17 play providers off against each other and build into
18 the contracts the kind of penalties that would produce
19 the service quality that they need.
20 But your question was how are Enterprise
21 customers different. I think they tend to buy
22 services over which they can exercise a little more
23 control in terms of data collection and responding to
24 outages because they map their own network
25 performance, so they may have more data about a

1 private network than the average mass market consumer
2 is going to have about their internet access.
3 MR. GOLDTHORP: You look like you're
4 wondering.
5 MR. BUGEL: I mean, we obviously deal with
6 Enterprises all the time, and as we discussed in the
7 earlier panel the customers are extremely
8 sophisticated in how they are negotiating SLAs.
9 MS. BOOTHBY: While the are negotiating. It
10 doesn't matter how sophisticated you are if your
11 competitive choices are limited you can't translate
12 that knowledge and sophistication into negotiating
13 leverage.
14 MR. BUGEL: So you're saying people should
15 invest in providing more competitive alternatives so
16 they can suffer higher nonperformance penalties?
17 MS. BOOTHBY: Well, I think there is a limit
18 to how much the Commission can assume that the market
19 will drive reporting and service quality corrections
20 in this environment.
21 MR. BUGEL: I think the Commission needs to
22 ensure marketplace where people have the incentive to
23 invest to provide your alternatives.
24 MS. BOOTHBY: Well, that's right and so far
25 looking at the kind of earnings most major carriers

1 are enjoying, that doesn't seem to be their problem.
2 MR. GOLDTHORP: Let me steer us back to the
3 public safety and homeland security, and one of the
4 things I definitely wanted to touch on before we get
5 to questions and answers from the audience is how we
6 get this data. We've talked about the kind of data
7 that we might be able to get. We did touch on one
8 thing that I was hoping that we'd have time for, maybe
9 we will later, and that's the routing infrastructure,
10 and if we don't talk on the panel, maybe offline.
11 But now, you know, we get data today through
12 a set of Part 4 rules that were established by rule,
13 obviously, and so the question I'm wondering about is
14 are there other things that we should be trying to
15 collect, are there other ways to collect the data,
16 other processes and systems that we should be
17 considering that would maybe minimize the burden?
18 Jim, I'm not asking you anything. I'm suggesting
19 something.
20 So that would minimize the burden but would
21 also result in the information coming in in a manner
22 that is most useful, Any ideas on that.
23 MR. KEECH: Well, I think to not take
24 advantage of the technology that's out there from an
25 automation reporting standpoint would be foolish. The

1 burden is around capture the data, massaging of the
2 data in the format necessary to report it, and then
3 actually reporting it, all of which have cost, the
4 latter being typically today data entry by a person
5 into an online system.
6 To the extent that you have surveillance
7 systems out there that are capturing this data out of,
8 you know, various providers' networks, either a part
9 of an alarm surveillance or performance reporting,
10 whatever the metric, to the extent any are determined
11 that need to be reported, there are ways to automate
12 that and eliminate or minimize the third cost of the
13 resources necessary to actually do the reporting.
14 What comes with that is the burden also then
15 to protect the integrity of that data down to the
16 service level or service provider format; some sort of
17 black box security so that if data is being reported
18 on an automated basis according to defined parameters,
19 that it is secure from those who are not authorized to
20 see it or use it.'
21 MR. WOUNDY: Right. I mean, depending on
22 what kind of data we end up talking about. I've been
23 involved in some projects where we've been trying to
24 share some -- at least limited amount of information,
25 one set of issues is confidentiality, competitive

1 issues. So you know, how is our network really
2 structured, et cetera. Those are things that we don't
3 necessarily want to have posted out in the internet.
4 I mean, we don't want to have a network map that says,
5 here, attack this router right here and you can take
6 out 40,000 people. That's kind of very
7 counterproductive.
8 But alongside the competitive and
9 confidentiality issues, depending on what we're
10 talking about, we could also start getting down into
11 consumer privacy issues. So there are a number of
12 ways that shows up. So if we were starting to gather
13 statistics on congestion on a per user basis, like how
14 much traffic are they generating, we'd have to be very
15 careful about anonomizing that kind of data.
16 So I mean, obviously if we were talking
17 like, you know, 1,350 DS3 circuits and some large
18 number like that, not getting down to individual
19 users, but sometimes when it comes to internet stuff
20 the kind of data you end up getting out is, you know,
21 a particular route or a particular customer or a
22 particular, you know, piece of traffic.
23 And so it's very important to make sure that
24 we maintain customer confidentiality as well. I mean,
25 we're obligated under law to do that. The Cable Act

1 of 1984 already says that. And so those are some of
2 the other considerations we need to have when we do
3 all this kind of reporting.
4 So when we've participated in these various
5 third parties like this ATLAS project, we've had to be
6 very careful that the kind of data that's being
7 emitted out of that system is not violating any
8 customer privacy issues because, you know, if you look
9 at the kind of probes that you have in the network
10 today, D-pack inspection, I mean, if you look at the
11 details there sometimes you're getting down to an
12 individual packet, an individual communication, you
13 know, because you need to know where the source of
14 this bautenent attack is coming from; you know, who is
15 in command and control, but at the same time you have
16 to still respect consumer privacy there because that
17 consumer that may be the source of this bautenent
18 attack may not be the witting participant in this, and
19 so you still have to, you know, do some level of
20 protecting their identity.
21 But I think, you know, in terms of like
22 public repositories, I means, that's certainly -- just
23 to give you some more ideas, we already talked about
24 ATLAS, we already talked about these looking glasses
25 out there that give you all the BGP routes. Just to

1 give you a third one there is measurement lab.
2 Now, measurement lab was founded by New
3 American Foundation and Google to drive us ISPs nuts.
4 I mean, sorry -- to measure what the congestion
5 looked like across our networks. But they've been
6 building this repository of information in terms of
7 different users that have gone to these different
8 measurement lab test probes they have, N-Pad and MDT
9 and Shipper Probe, and in the meantime -- these were
10 all build by academics, and in the background they
11 have been saving all this information into these
12 databases that they then plan to release with
13 anonymized customer data, of course, out to the
14 research community so that the research community
15 knows, you know, what's going on with respect to
16 congestion, how often does it happen, are there any
17 patterns or similarities between, you know, this ISP
18 customers and those ISP customers, is cable different
19 than DSL, different than fiber to the home. Those are
20 all kinds of other things that are going on there. So
21 there is another whole repository that's out there
22 where information is being collected, and for
23 measurement lab we didn't even have to do anything.
24 They just went off and built this on their own.
25 So definitely worth looking into what's

1 being collected today and I'm sure there is more
2 things. In terms of like all the commercial websites,
3 you have Neilson Online, and Keynote Systems, and Com
4 Scores, looking at all those things to see what does
5 it look like in terms of the experience that those
6 different sites for content and applications, you
7 know, how fast is it to get to Yahoo versus Google
8 today. And so there is yet another whole repository
9 of information that's out there, so some places to
10 start.
11 MR. GOLDTHORP: Thanks, Rich.
12 In addition, there is sort of a middle
13 ground. There is the -- well, there is always paper
14 filing. That's something we haven't been doing for a
15 long time. Then there is NORS which is the first
16 generation electronic filing. It still requires at
17 least, you know, human intervention in most cases,
18 people have to enter the data.
19 Then we've been talking about this idea of
20 the Commission getting access to data that's publicly
21 available, you know, at least to a point, and that
22 communication providers don't have to do anything for
23 us to get it because it's out there. Others are
24 making it available, so that's another.
25 But there is something in the middle and I'm

1 wondering to what extent your network operations
2 environments would enable sort of an electronic
3 bonding between systems we have here and systems that
4 communication providers' monitoring systems, alarming
5 systems that communication providers have, and data
6 aggregation systems that communication providers have
7 that already run algorithms today to do things like
8 alarm correlations so that you can correlate multiple
9 alarms to a single fiber cut. I mean, that's sort of
10 a physical error example, but there are others higher
11 up in the stack.
12 I'm wondering if technology has moved a pace
13 to the point where that sort of electronic bonding
14 solution would allow us to get useful information in a
15 more sort of expedited and more sort of in a way that
16 would be more error free in a sense, right.
17 MR. BUGEL: Yes, I think that is moving it
18 forward and I think there is one other step, and that
19 is when a rule or a metric is created, that rule or
20 metric has to be operationalized into the hundreds of
21 companies that fall under the jurisdiction of that
22 rule. So that requires some level of interpretation,
23 so you want to keep the subjectivity out of the
24 measure, you want to keep it purely objective, but
25 also you want to make it material. You want to make

1 that is something that is consistent, you want to make
2 it something that is consistent across the industry,
3 you want to make it something that is easily
4 applicable through the analysis suites that are bought
5 from the various vendors across the industry.
6 I think those are all things that lend
7 itself to less burdensome, and certainly filling out
8 paper forms is not where we need to go, and given the
9 complexities of these operations and given the
10 complexities of just what we've discussed today in
11 terms of network management and things that are going
12 on, it is more -- it is far more appropriate to have
13 those limited resources actually managing the problem
14 as opposed to filing a report.
15 So any level of automation actually helps
16 that. I mean, that is really the quest here. To the
17 degree of, you know, how intimate we would like to get
18 with that, that's really something up for debate, but
19 certainly I think that's going in the right direction.
20 MR. GOLDTHORP: Colleen, in your word, do
21 you have that kind of arrangements, contracts that
22 Enterprise customers negotiate with communication
23 providers today, is that sort of visibility generally
24 provided?
25 MS. BOOTHBY: It varies tremendously, but it

1 is available.

2 MR. GOLDTHORP: Okay. So depending on

3 what's on the SLA it can be done.

4 All right, we're about closing in on ten of,

5 and what I'd like to do now is -- unless there is any

6 closing comments anybody wants to make.'

7 MR. WOUNDY: Just one other thing. In terms

8 of e-bonding, the one other thing I think -- you know,

9 we, ISPs, need to go back and do some research to make

10 sure that we know what kind of trouble reports, what

11 kind of tickets would be appropriate to share. I know

12 that in some ISP environments a lot of things are done

13 manually, you know, entered manually, but e-bonding

14 would allow it to share it automatically.

15 In other environments there is all kinds of

16 tickets that are created automatically, and it's not

17 clear that, you know, if there is like, you know, an

18 issue impacting 10 customers or whatever, that you

19 really want all that information to be flooded over

20 the FCC.

21 And so I think maybe one other thing is

22 maybe to make sure that there is the right level of,

23 you know, thresholds applied to the e-bonding stuff

24 because for like a particular Enterprise, you know,

25 clearly any ticket open against an Enterprise, that

1 Enterprise will be interested in knowing this. If
2 you're the FCC, you don't necessarily want to know
3 about like all 15 million customers, so we need to
4 figure that out.
5 MR. GOLDTHORP: Yes, there is two separate
6 activities I can imagine. There is the process of
7 formulating the da ta model, and the data model is not
8 going to be the same as the thresholds that are set in
9 a communication provider's monitoring system for
10 action by -- you know, a truck or to -- no, we're not
11 interested in every time a truck hits the road.'
12 MR. WOUNDY: Yes, you do not what that.
13 MR. GOLDTHORP: I know and we don't get that
14 today with NORS, so I would see that as a different
15 activity from the operationalization that we would --
16 the best way to make it happen.
17 Okay, any questions from the audience?
18 Harold?
19 MR. SALTERS: I've got a question for
20 Richard.
21 MR. GOLDTHORP: To the microphone, please.
22 Thanks.
23 MR. SALTERS: I've got a question for you,
24 Richard. You mentioned performance metric over system
25 routers, and I just wasn't clear on whether that was a

1 product or a metric package or you called it --'
2 MR. WOUNDY: Sam Knows.
3 MR. SALTERS: Could you spell that out,
4 please?'
5 MR. WOUNDY: Sure. S-A-M K-N-O-W-S.
6 MR. SALTERS: oh, Sam Knows.'
7 MR. WOUNDY: Yes.
8 MR. SALTERS: And this is a proprietary
9 package?'
10 MR. WOUNDY: Yes, Sam would know. It's some
11 kind of a package. I think they target it to a Cisco
12 router, you know, It was probably because it was
13 whatever was available. I think they run their own
14 Linux distribution and it was easy to load that Linux
15 distribution onto Cisco routers. So you know, how
16 they picked Cisco or not is probably almost
17 irrelevant.
18 But Sam Knows is, believe it or not, a U.K.
19 company, and they work with OFFCOM and they have
20 deployed thousands of those Sam Know devices all over
21 the U.K. and they were using it to measure U.K.
22 broadband performance. So it's definitely been used
23 before. There was a Broadband.gov blog entry just
24 last Friday that announced that the FCC was going to
25 leverage some more technology in the U.S., and I think

1 they said that like they're going to start signing up
2 people in the next couple of weeks.
3 MR. SALTERS: So somebody from the U.K. this
4 is a project that is paid for by OFFCOM working with
5 Sam Knows?'
6 MR. WOUNDY: Yes, and I don't know the terms
7 of the FCC agreement -- well, we can ask some people
8 from the FCC.
9 MR. SALTERS: Would you care to comment,
10 Jeff?
11 MR. GOLDTHORP: Not right now because I
12 don't know. Jeff doesn't know.
13 (Laughter.)'
14 MR. WOUNDY: There is a blog entry and there
15 is a person's name. I just forget whose name it was.
16 MR. SALTERS: Thank you.
17 MR. GOLDTHORP: Yes?'
18 MR. WOUNDY: But it was somebody from the
19 FCC who would be a good person to ask.
20 MR. SALTERS: Thanks.
21 MR. GOLDTHORP: Any other questions? Sir?
22 MR. KILBOURNE: Brett Kilbourne, UTC. Our
23 members are utilities, and I was very interested in
24 your discussion about Enterprise customers. It's
25 certainly an issue for us. Our members have real

1 desperate need for reliable communications, and since
2 the discussion seems to be focusing on the IT part of
3 it, I wonder if you all could address the issue of
4 priority access because we really need to get reliable
5 communications instantaneously, especially during
6 times when there are emergencies, when the networks
7 get congested. So I was wondering if you could talk
8 about that, and also talk abut what latency rates
9 we're seeing when you see those spikes occur, just a
10 general question.'
11 MR. WOUNDY: By the way, would this be to
12 the home or would this actually be to like a utility
13 facility?
14 MR. KILBOURNE: To a utility.'
15 MR. WOUNDY: To a facility.
16 MR. KILBOURNE: For a smart grid, I mean, as
17 well.'
18 MR. WOUNDY: Okay.
19 MR. KILBOURNE: It cuts both ways.'
20 MR. WOUNDY: I don't think I would use cable
21 modems though.
22 MR. BUGEL: So are you talking about
23 emergency communications priority or are you just
24 talking about --
25 MR. KILBOURNE: We can go with that in terms

1 of voice.

2 MR. BUGEL: In terms of?

3 MR. KILBOURNE: Voice communications.

4 MS. BOOTHBY: Voice communications on

5 wireless?

6 MR. KILBOURNE: Yes.

7 MR. BUGEL: So right now under the circuit

8 switch environment it's WPS, that's the current rules

9 that exist, and basically through the NCS and through

10 the broadband plan there is going to be -- the FCC is

11 planning on working on packet switch priority in the

12 LTE or the next generation 4G environment. So right

13 now WPS is the priority protocol for the wireless and

14 basically utilities are included in that hierarchy

15 which I'm sure you're aware of.

16 Do you utilize WPS? Are your customers or

17 your clients --

18 MR. KILBOURNE: Some do, yes. I means, one

19 of the issues we have with that is utilities are

20 fairly low on the ranking, so that's one of the

21 concerns we have generally in terms of the WPS. But

22 in terms of negotiating, for example, an SLA, in terms

23 of getting priority access, is that something that

24 carriers support? How prevalent is it, and can you

25 give us a little insight in terms --

1 MR. BUGEL: Well, WPS is basically -- we
2 are, the carriers are an actual contractor to CSC,
3 which is contractor to DHS.
4 MR. KILBOURNE: Right.
5 MR. BUGEL: Basically they come to us. They
6 actually provide the service. So the rates are set by
7 the carriers and I guess I'm a little confused. Each
8 carrier has -- I don't know the exact rates of each
9 carrier, but it's a subscriber -- I think a lot of
10 carriers have dropped the actual monthly subscriber
11 fee, but there is a minute fee.
12 MR. GOLDTHORP: Are you talking about -- I
13 mean, one of the things I heard you ask was what can
14 be done to push utilities up in the priority a little
15 bit. In terms of getting priority service? There is
16 a tiered -- is that what you're talking about?
17 MR. KILBOURNE: For example, you've got a
18 Katrina type situation. You know, how could a utility
19 basically guarantee that its communications are going
20 to get through in that kind of a scenario when you've
21 got a congested network?
22 MR. GOLDTHORP: Right. Well, there is two
23 questions, right. There is getting priority service
24 to start with, right, and so there are priority
25 levels. When you go to get the service, right, there

1 are people at the top of that list, and I don't know
2 if utilities --
3 MR. BUGEL: Yes, there are five levels of
4 hierarchy that's set by the OSTP, and Executive Office
5 of the President that actually sets those, and
6 delegates those down to the NCS, John O'Connor, who is
7 actually sitting in the audience, is versed in this,
8 and probably could help you understand how you could
9 move around in the priority. We don't set those
10 rules.
11 MR. GOLDTHORP: That's probably something
12 you should talk to John and I about.
13 MR. KILBOURNE: But in terms of latency, you
14 guys are basically saying that you're monitoring at
15 all times. What kind of latency levels are you seeing
16 during these spikes that you're monitoring? What's
17 the high rate in terms of latency?
18 MR. GOLDTHORP: I don't really know. That's
19 my discipline. I'm not an engineer.
20 MR. KILBOURNE: Okay, I'll withdraw the
21 question.'
22 MR. WOUNDY: Well, latency on the wireless,
23 I mean, it's -- I don't know. On the broadband
24 network there has been issues on the broadband network
25 in terms of latency, but I don't think that really

1 applies in this case, but there was one time where you
2 could see several seconds of delay in the upstream,
3 which was completely ridiculous, and there was all
4 kinds of efforts to work around those issues because a
5 lot of it had to do with the -- either your DSL modems
6 or your cable modems, and bad assumptions they have
7 made.
8 I think on the backbone, backbone links and
9 regional access links, the speeds are so fast right
10 now that the kind of latency you see there is very,
11 very minimal. You hardly notice router hops anymore.
12 MR. BUGEL: I may have misunderstood your
13 question. On wireless network there is thresholds,
14 you can't complete a call and end a call unless it
15 reaches the thresholds in the network. Basically in a
16 circuit switch call if that latency is too long the
17 call won't complete; the same in the packet switch
18 network. But basically you manage that call -- you
19 manage those call thresholds so that you have less
20 than 1 percent blocking on either side of that.
21 So I didn't know you were talking
22 specifically about the wireless network.
23 MR. KILBOURNE: Okay, thanks.
24 MR. GOLDTHORP: I thought there was somebody
25 else that had a question. Yes, there we go.

1 MR. TAVARES: Tom Tavares from Expirix.
2 Getting back to the probe question, and I
3 guess Dave from Frontier had said, you know, getting
4 close to the customer, whether it be residential or
5 Enterprise is something that's difficult to do, and
6 then we talked about the cost of deploying the probes
7 and having to implement that would take time.
8 Now, there are other methods. You can use
9 standard-based methods. I'll just use VOIT, for
10 example. There is new standards, RTCPXR extended
11 reports, they can come and sip messaging and you
12 wouldn't need to put a probe out there. The device,
13 no matter what vendor it would be, if they have
14 implemented the standard, and it's been around for
15 about two years, you could get metric off of that and
16 there is metric that could be used by any service
17 provider, you know, Mausk, Peskor, R factor, jitter,
18 echo, round trip, delay and things like that.
19 Do you see implementing those and not having
20 to roll a truck out there or put a probe on the prem.
21 which would save a lot of money and time? And do you
22 see how the manufacturers have the end point devices,
23 the routers or the actual phones themselves, have they
24 implemented these technologies?
25 And of the Comcast gentleman, you've had the

1 loop-back technology for NCS protocols and SIP, but
2 you had mentioned where you don't want a million
3 people all calling at the same time or making a call.
4 Even though it doesn't ring the phone, it could be
5 affect the network, but these newer protocols like the
6 RTCPXR could be an answer without having to put probes
7 in. Are you looking at that type of technology at
8 this point?'
9 MR. WOUNDY: I think that technology can be
10 very useful when you're providing voiceover IP
11 service. The reason why I think there is interest in
12 the probes is the probe is measuring more than just
13 voice IP service, and it may be to a customer that
14 either is getting voice IP service from someplace else
15 or isn't getting that kind of service at all. Maybe
16 they're getting wireless service or something else.
17 So the point of the probe is to have -- it
18 does a couple of things for you. One is it -- the
19 alternative, the real alternative to using the probe,
20 and I'll come back to the RTCPXR stuff because I think
21 there is some promising stuff there, the real point is
22 having the probe is the alternative is to go to a
23 speed test site. So you go to speedtest.nav, or you
24 go to measureandlob.nav, or one of these places, and
25 you hit the bottom, the java button and some little

1 java program runs, and then it spits out some values
2 to you, and maybe those values are meaningful and
3 maybe they aren't.
4 A lot of the problems with not having those
5 probes is if I have malware on my computer, I'm
6 running a 8 to 11 B wireless network in the home, and
7 it's crap. I'm going off to some -- you know, to some
8 site across the internet like, you know, I'm going to
9 a measuring lab site and I think it somewhere in the
10 U.S. but instead I'm being redirected to Amsterdam.
11 All those things end up causing all kinds of bad
12 effects to the measurement results, and sometimes
13 you're really not measuring the ISP anymore, you're
14 measuring something else.
15 And so what's good about the probes is
16 you've eliminated the virus -- malware aspect. You've
17 eliminated -- you know, it's hard wired, it's some box
18 that just sits there and doesn't do anything, and it's
19 doing specific tasks periodically, not just when the
20 consumer says, gee, you know, it's 12:00, it's time to
21 do measurements. I mean, usually our customers aren't
22 that disciplined, and so the box can do that. The box
23 can be told your test time is noon, and somebody
24 else's test time is one, and that way you can get full
25 coverage without everybody beating up the network at

1 the same time. So there is a lot of interesting
2 things about the probes.
3 In terms of voice IP measurement, I think
4 there is a lot of good stuff in XR. I know that cable
5 labs is looking at that technology. I remember when
6 the Tulitian guys were reaching out to me probably --
7 it must have been five or six years ago, I think that
8 stuff is starting to get implemented. One difference
9 there is my impression of the RTCPXR reports is, you
10 know, that's the kind of data that would go to us, and
11 we would be able to measure it because we see the RTP
12 traffic and, you know, we're the recipient of that
13 whereas all these other mechanisms are over-the-top
14 mechanisms, so like the FCC could put out probes
15 without having to worry about -- you know, the probes
16 will go back and report back to FCC directly less, you
17 know, the FCC also runs a wipe service they're not
18 going to see the XR reports.
19 MR. TAVARES: All the probes we talked about
20 today they are all software-based aren't they? We're
21 not talking about putting boxes in.'
22 MR. WOUNDY: Well, with the Sam Knows stuff,
23 San Knows software, it goes on top of a fairly
24 standard home Gateway, and because it's not going on
25 your home computer, then you don't have to worry about

1 whether your home -- like I had a home computer that
2 was sitting in my office that I had no idea that it
3 was connected up via like 10 meg, and I was trying to
4 measure our 12 meg. service, and plus the computer was
5 crap.
6 I mean, you want to eliminate all of those
7 factors when it comes to testing, especially if you're
8 going to say, you know, I'm going to start making
9 decisions on this, like, oh, this ISP is under attack,
10 or, oh, this ISP is underprovision network. I mean,
11 if you're going to make decisions like that, you don't
12 want to make decisions on that based on, you know,
13 Rich has a 10 meg. hub that he bought 10 years ago
14 that he stuck in his office that's corrupting the
15 results.
16 So I think there is definitely value in
17 these XR reports. I think it probably makes more
18 sense in the context if we were doing voiceover IP
19 measurement. I think for general internet
20 measurement, maybe, but I'm not sure it's always
21 measuring the right thing.
22 MR. TAVARES: The point was rather than
23 having to put probes and multiple services putting
24 probes everywhere just using one probe maybe in the
25 core to just take measurements to avoid cost and

1 implementation and timeframe.

2 MR. KEECH: I think the point is what's that
3 probe talking to. There has got to be something on
4 the other end of a uniform nature to make results
5 across multiple providers mean something to the FCC or
6 any reviewing agency or organization. As I mentioned
7 earlier on in the conversation, there is conceptually
8 at least a point in the core that's launching the
9 probe, and then a recipient someplace in the network
10 which could in fact be to Richard's point, firmware,
11 software loaded on a CPA device, but it will take time
12 to standardize what those requirements are and then
13 have the firmware developed via the various
14 manufacturers, and there are literally dozens upon
15 dozens of those out there, to distribute that out to
16 get a complete and robust picture of a network.

17 MR. TAVARES: The electronic bonding piece,
18 we kind of refer to that in my company as enrichment
19 data from different resources, and more of leveraging
20 different third party resources that might already be
21 available to all service providers, we see that as the
22 key for anyone to monitor a true end to end type of
23 service flow, and I think that can be done with maybe
24 10 to 20 critical metrics that are already out there,
25 depending on what service you want to mention. It's

1 just a matter of getting the reports centralized and
2 baby sitting those and then alarming on those. Thank
3 you.
4 MR. GOLDTHORP: Thank you. Well, thank you
5 to our panelists, join me please in thanking them.
6 (Applause)
7 MR. GOLDTHORP: Appreciate you all coming.
8 Let me say a few words in closing now. I
9 first thank you all for coming, thank the folks that
10 joined us over the internet. Hopefully the session
11 today was useful to you. We covered a lot of ground.
12 Two issues that figure prominently in the national
13 broadband plan, the survivability and resilience, and
14 information collection, and we answered a lot of
15 questions today, and I learned a lot. So thank you
16 for coming. Have a safe trip home and hopefully we
17 will see you here again for another one of these in
18 the near future. Goodbye.
19 (Whereupon, at 12:01 p.m., the meeting was
20 concluded.)
21 //
22 //
23 //
24 //
25 //

REPORTER'S CERTIFICATE

DOCKET NO.: --

CASE TITLE: Critical Infrastructure & Information Collection

HEARING DATE: April 13, 2010

LOCATION: Washington, D.C.

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

Date: April 13, 2010

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