

UNITED STATES OF AMERICA
FEDERAL COMMUNICATIONS COMMISSION

NATIONAL BROADBAND PLAN WORKSHOP
CYBER SECURITY

Washington, D.C.

Wednesday, September 30, 2009

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

1 PARTICIPANTS:
2 Welcome:
3 COMMISSIONER MEREDITH ATTWELL BAKER
4 Panel 1:
5 JAMES ARDEN BARNETT, JR.
6 Rear Admiral (Ret.)
7 Chief, PSHSB
8 JOHN NAGENGAST
9 Executive Director, Strategic Initiatives for AT&T
10 Government Solutions
11 RICHARD PETHIA
12 Director, CERT, Carnegie Mellon University
13 DON WELCH
14 CEO & President, Merit Network, Inc.
15 Panel 2:
16 JEFFERY GOLDTHORP
17 Chief, Communications Systems Analysis Division,
18 PSHSB
19 MARC DONNER
20 Engineering Director, Google Health, Google
21 Finance, AdWords Engineering
22 DALE DREW
23 Vice President for Security, Level 3
24 ANDY OGIELSKI
25 President, Renesys Corporation
26 PHILIP REITINGER
27 Deputy Undersecretary, National Protection &
28 Programs Directorate, Department of Homeland
29 Security

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

1 PARTICIPANTS (CONT'D)

2 ALLAN SADOWSKI
IT Director, North Carolina State Highway Patrol

3 Closing Remarks:

4 JENNIFER MANNER
5 Deputy Bureau Chief, PSHSB

6

7 * * * * *

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

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

2 MS. MANNER: Good morning, everyone.
3 Welcome to our Cyber Security Workshop today. I'm
4 going to turn the microphone over to Commissioner
5 Baker who is going to open our event today. So
6 with that, thank you very much, Commissioner
7 Baker, and thank you everyone for joining us.

8 COMMISSIONER BAKER: Thank you,
9 Jennifer. And thank you all for being here. This
10 is such a critical workshop. I'm just thrilled
11 that we're hosting it. So, first of all, good
12 morning. And welcome to everyone for being here.
13 And this is the Cyber Security and Broadband
14 Workshop. I'm really happy to be -- have the
15 opportunity to be able to kick off this event
16 because I think it is so critical and so
17 important. You know, we said a lot about this
18 yesterday, but broadband has really become
19 critical infrastructure and it is the enabling
20 technology for the future of our children's
21 education, the next generation of health care,
22 smart energy grid development and public safety.

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

1 According to one metric, which I use a lot, it is
2 one-sixth of the economy upon which the rest runs.
3 So, a twenty-first century communications
4 infrastructure is essential for restoring
5 sustained economic growth, opportunity and
6 prosperity for our country. And as you all know,
7 the Commission will play an important role in
8 making sure that we get the right regulatory
9 environment. We need to make sure that we create
10 incentives for companies to build out
11 infrastructure faster, to reward innovation and
12 investment and to encourage competition so that
13 American consumers can have access to and can
14 afford the world's most advanced communications
15 systems. However, as society grows ever more
16 dependent on broadband -- did we lose our cyber
17 world? As societies grows ever more dependent on
18 broadband and as our traditional platforms are
19 increasingly more open and interconnected with the
20 internet, we become more susceptible to cyber
21 security threats. In fact, the number of security
22 breaches on the computer and communications

1 systems increases daily. Because the potential
2 for harm to communication systems due to cyber
3 attacks is so immense, I firmly believe that
4 network security is the most important issue
5 facing the communications industry. Consumers
6 expect and need reliable and secure broadband
7 infrastructure to distribute information and to do
8 our banking and to make investments and everyday
9 purchases. Most sectors of our economy routinely
10 rely on the durability and the security of IP-
11 enabled communications networks to securely
12 collect and move large quantity of data broadband
13 systems and are also a critical component of our
14 national defense and emergency preparedness. So,
15 attacks on communications infrastructure can
16 result in severe harm ranging from identity threat
17 -- theft -- easy for me to say -- to the
18 disclosure of sensitive and proprietary
19 information to service degradation and destruction
20 for all users, including public safety entities.
21 Cyber security is critical to ensure confidence in
22 the use of any network, whether wired or wireless.

1 And without such confidence we lose significant
2 foundation of our economy and homeland security
3 capabilities. If we do not get it right, it could
4 derail all of our other broadband efforts. So the
5 Commission has a part to play in ensuring that our
6 communications infrastructure is secure and I am
7 pleased that we are continuing to focus on the
8 importance of cyber security. To this end, the
9 Commission has already engaged in reviewing its
10 own needs and reaching out to industry and other
11 government agencies to address network security
12 issues and to enhance our awareness and our
13 ability to respond to cyber attacks. I would like
14 to take just a few minutes to acknowledge some of
15 the initiatives that are active -- that we are
16 active in the cyber security area. Cyber security
17 is not the only issue for companies that we
18 regulate, but also for the Commission itself. I
19 applaud Chairman Genachowski's initiative in
20 ordering a 30 day review of the Commission's
21 preparedness for major public emergencies. This
22 review, which the Chairman announced almost

1 immediately after being sworn in, resulted in a
2 report that was issued earlier this month that
3 discusses, among other things, the ability of the
4 FCC to prevent, monitor, detect and analyze cyber
5 attacks and recommends areas for improvements that
6 can be made. I encourage the Commission to
7 institute procedures to protect and respond to
8 attacks on its own networks and hopefully we can
9 lead by example. I am also encouraged by the
10 creation of the Commissions Inter Bureau Cyber
11 Security Working Group to evaluate our role in
12 network security, assess a need -- assess the
13 needs and the requirements for cyber security
14 expertise and assets and to identify
15 vulnerabilities. This working group will deliver
16 a report to the Chairman by the end of November,
17 with specific recommendations to address
18 deficiencies. We should also continue to engage
19 with industry to develop best practices to secure
20 networks against intrusions. The Commission has
21 taken positive steps in the past by chartering and
22 working closely with the Network Reliability and

1 Interoperability Counsel -- a Federal advisory
2 committee composed of private sector
3 representatives that we established to develop
4 best practices for ensuring reliability and
5 resiliency in the telecommunications networks.
6 NRIC issued an extensive series of more than 200
7 industry best practices aimed at improving network
8 security. This work will be continued by the
9 Communications Security Reliability and
10 Interoperability Counsel, which was recently
11 rechartered to review and update the cyber
12 security best practices and to take into account
13 the new and advanced technologies including
14 broadband and IP-based technologies. The
15 Commission is also providing outreach and
16 education to encourage the implementation of cyber
17 security measures. We should continue to
18 collaborate and assist industry to develop the
19 tools, the technologies to protect infrastructure,
20 to restore and recover networks after cyber
21 attacks. The Commission should also pursue
22 policies that foster innovation and investment in

1 securities technologies for communications
2 networks and have procedures in place to aid
3 industry members and the public safety community
4 to recover from network intrusions. Congress has
5 instructed us to develop and implement a national
6 broadband plan and that is why we are here. By
7 February 17 of 2010 we must and will deliver a
8 plan to Congress that will seek to ensure that
9 every American has access to broadband capability
10 and establishes clear benchmarks for meeting that
11 goal. In formulating that plan, we need to
12 consider how to secure broadband networks. The
13 Commission is off to a good start by requesting
14 comment on public safety and Homeland Security
15 concerns and specifically on cyber security. Over
16 the past several weeks, we have had numerous
17 workshops on a variety of topics. We heard a
18 variety of feedback yesterday. And so this is
19 going to assist us the national broadband plan.
20 And today we look to the public safety community,
21 the government agencies, the academia and industry
22 to provide their expertise on this very important

1 topic of cyber security. These two panels will
2 discuss the ability to prevent, detect and respond
3 to attacks and to consider how broadband
4 technologies, tools and innovations can assist
5 efforts to secure the nation's critical
6 communications infrastructure. I really
7 appreciate you guys for being here. I appreciate
8 your work and your expertise. As I mentioned
9 before, I think it's so critical that we get this
10 right, because if this is the part we get wrong,
11 all the rest is for naught. So, that said, I
12 would like to introduce Admiral Jamie Barnett. He
13 is incredibly capable and we are so lucky to have
14 him as the Chief of the FCC's Public Safety and
15 Homeland Security Bureau. So he is going to
16 introduce you and moderate the first panel. So,
17 welcome.

18 ADMIRAL BARNETT: Good morning and
19 (inaudible) thank you for being with us this
20 morning and for your emphasis and leadership in
21 this area. And thank you all for being here. My
22 name is Jamie Barnett. I'm the Chief of the

1 Public Safety and Homeland Security Bureau for the
2 FCC. We have arrayed before you, from the murky
3 world of cyber security, the good wizards who are
4 going to -- to lead us forward in what I think is
5 going to be a very interesting and important
6 discussion. I'm going to introduce our government
7 participants first. On the far side, Jon Peha is
8 our Chief Technologist for the Federal
9 Communications Commission. Next to him is Richard
10 Hovey, a Telecommunications Specialist who is
11 actually in my bureau and our expert in this area.
12 And then next to him, Robert Cannon, who is the
13 Senior Counsel for Internet Law for the Office of
14 Strategic Planning for the FCC. We appreciate
15 them being here. Now coming to this end and right
16 next to me, I have John Nagengast, who is the
17 Executive Director for Strategic Initiatives for
18 AT&T's Government Solutions. Mr. Nagengast's work
19 at AT&T focuses on their corporate capabilities to
20 resolve national security problems facing defense
21 and intelligence communities. Before working at
22 AT&T, he was with the National Security Agency for

Phone (703) 519-7180 Fax (703) 519-7190

1 38 years and last served as Principal Director for
2 Corporate Strategy, where he led the NSA to
3 develop strategic relationships with U.S.
4 industry. He was also responsible for
5 coordinating industrial relationships across the
6 intelligence community. In addition, he served
7 previously as a member of the Cyber Security
8 Commission for the forty- fourth presidency and
9 you may remember that they issued a very important
10 report. Next to him, we have Richard Pethia, who
11 is the Director of CERT at Carnegie Mellon
12 University. CERT's mission is to identify,
13 develop, apply and broadly transition new
14 technologies and practices to improve security.
15 He was awarded the position of Software
16 Engineering Institute Fellow for his vision in
17 establishing the CERT program. He has also served
18 as the Director of Engineering at Decision Data
19 Computer Company, where he was responsible for
20 engineering functions and resource management.
21 Mr. Pethia has testified before the U.S. Congress
22 numerous times on cyber security issues. And

1 last, but by no means least, we have Don Welch,
2 President and CEO of Merit Network, Inc. Merit
3 was formed in 1966 to design and implement a
4 computer network among public universities in
5 Michigan, which has expanded to include other
6 states. Prior to his work at Merit, Mr. Welch was
7 the Director of Enterprise Technology and
8 Merchandising Applications at H-E-B retailer. He
9 also served in the U.S. Army for 25 years,
10 retiring at the rank of Colonel. His last
11 assignment in the Army was as the Associate Dean
12 for Information Technology and Professor of
13 Computer Science at the United States Military
14 Academy at West Point. As you're aware, today's
15 workshop will examine the nation's ability to
16 prevent, detect and respond to cyber attacks and
17 how broadband technology can enhance our nation's
18 cyber security efforts. We will also take a look
19 at the challenges that broadband technologies can
20 bring to cyber security efforts. This panel will
21 focus on broadband technologies, tools and
22 innovations and how they can aid in preventing

1 cyber attacks on our critical communications
2 infrastructure. So, at this point, let us begin
3 with a presentation by each panelist. And we'll
4 start with John Nagengast of AT&T.

5 MR. NAGENGAST: Okay, well, thank you,
6 Jamie and thank you to the FCC for giving myself
7 and the other panelists here the opportunity to
8 talk to you a little bit about cyber security.
9 It's a topic near and dear to me. I'm going to --
10 I'm going to start out by talking a little bit
11 about what we do at AT&T in terms of how we
12 protect our network infrastructure and our
13 customer base. We take cyber security very
14 seriously and some of the complexities associated
15 with that problem and then maybe a few thoughts on
16 broadband and how broadband and cyber security
17 relate to each other. So we'll see. I think I
18 got the button here and it works, actually. This
19 is the definition we use for cyber security. And
20 the point here is that cyber security is not a
21 single thing. It's not an appliance that I can
22 plug in someplace or a piece of software that's

1 going to make me secure. It's the whole process
2 end-to-end, looking out across the whole network
3 infrastructure from the IP core out through all
4 the access media and it's a whole process that
5 we've implemented within AT&T as part of our whole
6 process of making sure we have a reliable and
7 resilient and secure services to our customer
8 base. Every -- you know, this is a very complex
9 problem. And every time I think I understand it,
10 something else comes along that I've never heard
11 of before and adds a new dimension -- new
12 dimension to the problem. But, I think you're all
13 familiar with some of the -- some of the aspects
14 of this. The end platforms and the application
15 software continually process of finding bugs and
16 patching and fixing and it's just a continuing
17 saga. And I know there's efforts within the
18 industry to try to make that a little better, but
19 we still have along way to go obviously between
20 the -- that the end system well and making this --
21 the hardware and software more secure. Just
22 managing the whole -- the whole infrastructure

1 really challenges the users, the system
2 administrators, cyber security experts. Really
3 every day you're really challenged to understand.
4 You know, how do I configure this platform? How
5 can I make it the most secure? And even then,
6 it's not -- it's not totally secure and we're
7 always finding ways that somebody can get into a
8 -- a different piece of the infrastructure. The
9 speed and the threat is rapidly advancing. Zero
10 day attacks, which is when somebody announces a
11 vulnerability and a patch that needs to be
12 implemented in a product and three hours later you
13 start to see exploit code emerging on the
14 internet. And it doesn't take long before that
15 exploit code is up and running and starting to do
16 bad things. Users simply cannot cope with the
17 continual stream of patches. There's a lot of
18 work been done in automating and advancing the way
19 we keep the software updated, but still a very,
20 very complex and difficult process. And again
21 it's very difficult for the users, the system
22 administrators that work the technology every day,

1 to keep up with the whole -- the whole process.
2 What we do in AT&T, we start with our core
3 infrastructure and we're largely converged around
4 an IP core today and moving all the various pieces
5 that -- of the new AT&T from Cingular Wireless and
6 other parts of the company onto that IP core. And
7 basically, our first line of defense is to watch
8 what's happening in the core from a statistical
9 basis. We look at ports and protocols and on an
10 individual basis. And how has this changed from
11 yesterday? How has this changed from the week
12 before? And we find very, very -- by looking at
13 it -- a very fine grain statistical analysis. We
14 can see things happening in the network in the
15 early stages. The other thing we do is look for
16 exploits around known attacks. And again every
17 time somebody announces a vulnerability or a patch
18 in a product, we start watching for exploit code
19 that's going to be going after that particular --
20 that particular -- that particular vulnerability.
21 We develop some very sophisticated capabilities to
22 identify those early on. What you want to be able

1 to do is identify exploit code that's emerging
2 before it actually gets it right and starts
3 actually affecting end user systems and we've
4 become very good at being able to do that and
5 catching it in its early stages and then figuring
6 out how we're going to mitigate that. We're
7 always striving to automate the whole process so
8 we can detect and mitigate in an automated
9 fashion. But, like I said earlier, everyday
10 there's something new and so the analysts are
11 always on the floor trying to figure out, hey,
12 this is something we've never seen before. What
13 is it? What's happening? Where's it coming from
14 and how do we go about protecting our
15 infrastructure, our customer base from that
16 particular exploit? This is just something we've
17 developed over time and we use this. This is the
18 tool that our security analysts use. We've
19 developed a sophisticated portal and it's
20 integrated with our whole operations management
21 capability. Again, looking at different --
22 different trends, what's happening. We watch what

1 happens when American Idol comes on and we see
2 spikes in traffic with SMS and texting and things
3 like that. But that's -- and that's kind of
4 normal behavior in the network. But we see other
5 surges of things which could be a distributed
6 denial of service attack taking place. We see
7 attacks against network infrastructure, like the
8 domain network -- domain -- excuse me, the domain
9 name system that happens all the time. And those
10 attacks are getting more frequent and more
11 sophisticated. So, again from a complexity
12 standpoint, it's everything from the top
13 infrastructure down to the end systems and
14 everything in between. And that's the challenge
15 we all face as we're trying to think about how do
16 we enhance cyber security from a national
17 perspective, how we integrate it into the
18 broadband strategy. And last but not -- and this
19 is just an example of our tool -- one of the tools
20 we use. We track about 60 botnets in real time
21 everyday. This just happens to be Confiker on the
22 first of April, which was April Fools Day. That

1 was the day it was supposed to do whatever it was
2 going to do and as you can see there's lots of red
3 circles, which means these are all computers that
4 have been taken over by Confiker or infected by
5 Confiker. But there's no yellow, which means
6 there's no controllers active and nothing happened
7 that day, which was good news for everybody. But
8 it's still out there and it's still continuing to
9 morph and get more sophisticated. So we don't
10 know -- nobody knows what the end game is with
11 Confiker. But again it's part of that continuing
12 process of seeing what's happening out there and
13 adopting to do threats as they -- as they evolve.
14 And last, but not least, I'd just like to close
15 with a few thoughts about what do we need to do in
16 the context of a broadband strategy. Obviously,
17 security and education and awareness is critical.
18 There are so many people that just don't
19 understand the cyber security challenge. It's
20 very difficult to keep up with all of it. We see
21 the market -- you know, developing market demand
22 based on that education and we really need to spur

1 innovation investment in providing cyber security
2 as a part of the broadband roll out. That needs
3 to be integral to the thinking of -- if we're
4 going to do broadband, cyber security has to be a
5 part of that. We believe managed services are
6 going to be the future. Again, it's too complex
7 for the user or the typical system administrator
8 to keep up with and we really need to simplify the
9 whole user experience from a security perspective.
10 We can't expect the user to say, well, I got this
11 icon that popped up says click here and we'll save
12 you from the latest threat. That just doesn't
13 work and we need to automate that whole process
14 and provide solutions that the users can cope
15 with. And that's my -- I'm over -- ten seconds
16 over. Thank you.

17 ADMIRAL BARNETT: Alright. John, thank
18 you so much. We appreciate that. Next, we'll
19 hear from Richard Pethia from CERT at Carnegie
20 Mellon University.

21 MR. PETHIA: For the last 20 years or
22 so, we've looking at the security problem.

1 Fortunately, we have better hardware -- securing
2 the microphones (inaudible).

3 ADMIRAL BARNETT: Right. That's tough.

4 MR. PETHIA: And it's been a challenge
5 over the 20 years to deal with a problem that's
6 constantly changing. This quote from General
7 Shelton is one that's similar to a number of
8 statements you've seen come from senior government
9 and business officials over the last -- especially
10 the last two years. There's a growing recognition
11 of the seriousness of the problem, the
12 pervasiveness of the problem and you're seeing
13 more and more organizations -- both inside and
14 outside of government -- that are trying to --
15 trying to take steps to deal with a serious issue.
16 One of the things I don't think is so widely
17 understood is just how complex this problem really
18 is. We have millions and millions of systems
19 connected loosely together into millions of
20 networks that are again loosely connected together
21 by nothing more than, in very many cases, loose
22 agreements to share common signaling conventions

1 and common protocols. There is nobody in charge
2 of this global information grid that we've put
3 together. The technologies that we use are
4 littered with vulnerabilities. We see new reports
5 of vulnerabilities every day -- literally
6 thousands of them every year -- and we have
7 technologies that come from who knows where, from
8 thousands of different vendors of unknown
9 prominence and there's always a concern about
10 supply chains that may be somehow corrupted
11 because people are trying to plant malicious code
12 in some of our devices. It's an ultralarge
13 system. It's open. It's dynamic. There is no
14 central administrative control. There is no
15 global visibility if you look across the whole
16 thing. And while we have a number of techniques
17 that are effective at protecting individual
18 networks and systems, we still haven't come to a
19 good job of understanding how to protect this
20 global infrastructure. As John said, we see new
21 kinds of attacks literally every day and in many
22 cases, our attack technology is outpacing our

1 ability to defend against those attacks. There
2 are a growing body of cyber attackers and what I
3 call cyber mercenaries -- guns for hire -- who
4 will, who will to the highest bidder sell their
5 services and their attack technology and we are
6 certainly seeing a number of Confiker, for
7 example, large scale -- at least the potential for
8 large scale coordinated attacks. On top of all of
9 that, we have a workforce that is woefully
10 inadequate in terms of the number of skilled
11 individuals that we need to deal with this problem
12 globally. There is a short supply. There is no
13 good, rapid way to accelerate the training of
14 these organizations. There are a limited number
15 of organizations that provide training and there
16 is still a lack of understanding of the complexity
17 of some of these issues. Certainly one of the
18 things to consider is whether or not we should
19 have a strong defense on the part of the
20 organizations that provide services to this
21 communications community. The answer is certainly
22 yes. But we have a dilemma. While the service

1 providers need to maintain a robust and secure
2 communications infrastructure, that same robust
3 communications infrastructure that delivers
4 services to their clients, also delivers attacker
5 bits to the targets on the end points of the
6 system. So, the tool that we use -- that we're
7 trying to protect is the same tool that the
8 attackers use to try to accomplish their means.
9 So I think we have a special challenge in this
10 case of dealing with both of those situations. A
11 question posed to us as panelists was, you know,
12 should there be some attention paid to having
13 service providers conform to a baseline set of
14 standards. And I think certainly those standards
15 are useful. They're important. But again, I
16 think it's important to understand the complexity
17 of the problem. Operational risk management
18 really requires harmonization a number -- of a
19 number of different kinds of activities --
20 security planning and management, business
21 continuity and disaster recovery, IT operations
22 and service delivery. And over the years, there

1 have been a number of good pieces of work done --
2 both inside and outside the government -- that
3 have set a strong foundation for codes of practice
4 that address each of those particular areas. And
5 I think there's certainly no need to go back and
6 reinvent all that good work. It's there for us to
7 harvest and take advantage of, but it's important
8 to put it together in the right ways. And so, one
9 of the things that we've done over the last couple
10 of years is looked at all of these codes of
11 practice, taken a step back and viewed how they
12 interact with one another and how they overlap.
13 And as you see from this diagram, you can take all
14 of those codes of practices, clust them together
15 into about four different areas of work, where
16 there really is a lot of commonality across the
17 various standards. So, that's the good news. A
18 lot of good work has been done. People are
19 beginning to understand how to put all of this
20 together, but the added level of complexity is
21 that it's important to understand this needs to be
22 not seen as a set of controls that are static --

1 once implemented, things are fine. This has to be
2 a very dynamic process. So what we really need to
3 measure is not just does an organization have the
4 right practices, policies and controls in place,
5 but can that organization sustain those things in
6 times of crises. And we don't really have good
7 ways to measure that, but that's really the
8 measurement that we need to try to get to because,
9 as was said by John, this problem changes every
10 day. It's critical that organizations have a
11 dynamic defense -- one that stays on top of the
12 changing complexities of the problem, be it come
13 from the attacker side or from new technologies
14 being introduced into the network that are going
15 to be vulnerable in their own ways. The other
16 thing that I wanted to mention just briefly, is I
17 think also service providers need to consider how
18 they support their customers and how they support
19 this global ecosystem that we've come to rely on
20 in so many different ways. Raising awareness and
21 understanding, I think, is a role that service
22 providers can play. They do have a direct channel

1 to their customers. There's ways to get
2 information out to them. In some cases, even
3 alerts and warnings of new kinds of attack if
4 that's appropriate. Participating actively in the
5 defense of the overall ecosystem, not just the
6 defense of their own infrastructure. My examples
7 here come from the IP world, but we certainly know
8 that IP address spoofing is a problem and we could
9 filter out a lot of those packets at the edges
10 before they even get into the system. We know
11 that it's necessary for network service providers
12 to provide support when organizations are being
13 crippled by denial of service attacks. But very
14 often the organization that's being attacked is at
15 the long end of a chain and what we really need is
16 to back up many steps upstream to be effective
17 with those filters. And finally, I think there's
18 opportunity for service providers to provide
19 managed services to their customers as a way to
20 take that small amount of expertise that we do
21 have and get it to be used in an effective way for
22 all of us. So, thank you.

1 ADMIRAL BARNETT: Thanks, Richard.

2 Next, we'll hear from Dr. -- Colonel Don Welch of
3 Merit Network, Inc.

4 MR. WELCH: Thank you. So, I'm going to
5 talk a little bit from my perspective as
6 ex-military. And I think before we can start
7 thinking about how to defend, we really have to
8 think about who we're defending against. And so I
9 think the big thing to understand is that
10 different from a lot of other types of problems
11 that we deal with, is that we're dealing with
12 people. They're people with some type of
13 malicious intent and they have a combination of
14 capability and intent. And we have to understand
15 what we're trying to do. So if I think about
16 classifying the types of people -- and this is
17 just a short list -- that might want to do us harm
18 in cyber space, certainly there's the state
19 agencies and those people may, in fact, at some
20 point want to cripple certain aspects of the U.S.
21 They may want to perform espionage and they have
22 better capability of doing it than anyone else.

1 Defending against them is going to be extremely
2 hard -- bordering on impossible, I would guess.
3 We've also got criminals and criminals, of course,
4 you know, they're after big money. They have a
5 lot of resources and they're going to use
6 different types of techniques to -- if you go for
7 personal gain. But, generally like a parasite or
8 a virus, they don't want to bring the system down.
9 They just want to profit from it. Certainly in
10 this day and age, we have to worry about
11 terrorists and terrorists have -- in some sense --
12 have same motivations that a hostile government
13 might have against us, although they don't
14 necessarily need to destroy us so much as they
15 need to bring notoriety to themselves, cause fear
16 and panic in our organizations. And I think we
17 can't also neglect the kind of pseudo-government
18 organizations like we saw after the -- the
19 incident with the P-3 Orion and the Chinese jet --
20 fighter jet -- where the Chinese computer clubs
21 that are sanctioned by the government came out and
22 caused a lot of harassing problems for us.

1 They're not necessarily controlled by the
2 government, but they do act in accordance with the
3 -- with what the government is trying to do. And
4 then, of course, you know, the largest thing are,
5 you know, what we call hobbyists or hackers or
6 whatever and they're going -- they have different
7 types of capabilities and different types of -- of
8 what they're -- needs that they're trying to
9 fulfill, such as notoriety. So, keeping that in
10 mind then, security is, of course, an engineering
11 problem. The volume of the triangle is basically
12 going to be constant. If you want more security,
13 it's going to cost us more and our systems are
14 going to be less useful. We want more usefulness;
15 we're going to have to lower security. So we've
16 got to come up with the right balance in our
17 system and I think the real difficulty in the
18 commercial world is it's very difficult to point
19 to an ROI. So, if we're successful, nothing
20 happens and that's -- that's kind of difficult.
21 How do you assess what the cost is? What's the
22 return for the investment for a commercial

1 provider? And as we know, in broadband, right now
2 it's a -- it's perceived as a commodity. A
3 connection is a connection. And people want to
4 pay the lowest price and if you come to someone
5 and say yep, I've got a more secure network than
6 them, so you're going to pay 20 percent more,
7 they'll be, well, gee, that would be great. But
8 -- especially in this day and age -- they can't
9 afford it. So -- so I think it's very important
10 that we think about a defense in depth because if
11 we look at our adversaries -- the people that are
12 coming against us -- they're very mixed. They
13 have a lot of different types of capabilities and
14 motivations. So there's no -- there's going to be
15 no single solution. It's got to be a combination
16 of things. And the most important thing, I think,
17 there is the quality of the people and the people
18 have to be motivated and they have to be trained
19 because they're going to have to outthink our
20 adversaries, because as my colleagues have said,
21 this is a really dynamic environment and it's --
22 it's not dynamic in a random way. It's dynamic in

1 that our adversaries are going to find the flaw
2 and they're going to get -- they're going to get
3 to us. So, when I've given talks before, I've
4 talked about the blazing saddles defense. And if
5 you remember Sherriff Taggart going through the
6 desert, coming up against the toll booth and
7 having to turn around and go back and get dimes
8 before he could pursue the heroes, many of our
9 cyber defenses are that way. We'll put up a
10 strong defense right here, and if our adversaries
11 are just a little smart, they'll just go a little
12 bit to the right and go around it and a lot of
13 security measures that I've seen tend to act that
14 way and we've got to remember that these people
15 are very smart and very adaptable. So, to finish
16 up, what I'd -- what I'd like to say is that from
17 a -- from a Federal Government perspective, we
18 really can't mandate, I think, how we're going to
19 defend. That -- that I'd think could be very -- a
20 difficult, if not impossible, solution. I have a
21 lot of experience in the Department of Defense and
22 the difficulties the Department of Defense has

1 with its somewhat homogenous mission and makeup of
2 people and being able to mandate the things that
3 will be done to defend the network. I think what
4 we've got to do is take allowances of all the
5 different types of situations that exist in the
6 vast complexity of the ecosystem and motivate
7 those people to come up with the best solutions --
8 the best defense solutions. And really that means
9 mandating results. How are you going to mandate
10 results? Well, that's another hard question, but
11 certainly full disclosure would be one. Right
12 now, there's no mandate that I know of to disclose
13 a security incident. Another problem defining
14 exactly what is a security incident that must be
15 disclosed. But if it was disclosed, you take a
16 step towards being -- coming up with this return
17 for the investment. If I can say specifically
18 that my network is more secure than your network
19 to people that are -- that it's important to --
20 they'll pay more for it and I can get some
21 justification for investing in the security there
22 if there were fines or so forth associated that

1 might work. My experience at H-E- B retailer was
2 it was very easy to get support to fix our credit
3 card system when the PCI standards came out from
4 the credit card industry that said we're going to
5 fine you \$50,000 a month unless you comply with
6 our system. And I could go to the senior
7 executives of the company and say it's going to
8 cost us \$300,000 to fix it, but we have to pay a
9 fine of \$50,000 a month if we don't. They go six
10 month ROI. That's an easy choice and we could
11 spend the money. But -- but coming up with that
12 return is really what's going to be hard for
13 commercial industry. Thank you.

14 ADMIRAL BARNETT: Don, thank you so
15 much. And, gentlemen, thank you for these key
16 insights. We've reached the portion now where
17 we'll have a conversation. Questions can come
18 from our government panelists from the audience
19 here and also from people who are here virtually
20 through -- through Webinar Webcast -- and may be
21 able to send. Hopefully they are with us through
22 broadband technologies, so they can have a good

1 use. But, now I would open it up to those
2 questions. John, you can go first if you like.

3 SPEAKER: Sure. Well, I was impressed
4 to see pictures of -- global pictures of the worm
5 spreading. If you're going to use -- I mean one
6 of the methods you talked about, for example, to
7 see security threats is anomaly detection. That
8 requires knowing what's happening in real time.
9 It also requires knowing something about the
10 baseline and you need to have a picture of the
11 world in order to do that. What I'm -- what I'm
12 wondering is are there organizations -- whether
13 it's AT&T or CERT or others -- are you comfortable
14 with the extent to which you can view what is
15 happening in real time on the internet to -- to
16 see threats as they emerge? And, if not, are
17 there -- are there things that might be done in
18 general -- particularly government might do -- to
19 help facilitate that?

20 SPEAKER: That's a great question
21 because everybody's got a picture. I see a couple
22 colleagues from Verizon and Quest out in the --

1 out in the audience -- and they have a cyber
2 picture and AT&T has a cyber picture and CERT has
3 a cyber picture and the -- I could name a dozen,
4 dozens of places where you can go and get a cyber
5 picture. But there's no unification of that today
6 and some of that is due to proprietary,
7 competitive reasons. And some of it's due because
8 there is no structure for -- for sharing that.
9 There are sharing mechanisms that exist today, but
10 it's more, you know, after the fact. What did you
11 see? We were attacked last night. Did you get
12 attacked last night? And you're never going to
13 solve this problem over the telephone is they way
14 I like to describe it. So there are things, I
15 think, we need to think about from a national
16 perspective -- that how do we create this common
17 operating picture in cyber space that will enable
18 all of the participants and all of the defenders
19 to do a better job of the defending because you
20 can see more of -- and obviously the more you can
21 see and the more you can attribute where an
22 attack, for example, is coming from -- which is

1 one of the great technical challenges today -- the
2 better off we're going to be able to defend our
3 national infrastructure.

4 SPEAKER: Would that indicate a
5 different structure for the information sharing
6 structures that we have now -- the ISACs
7 (inaudible) --

8 SPEAKER: Well, again, I think the ISACs
9 are a good vehicle. But again more of an after
10 the fact process as opposed to --

11 SPEAKER: Real time.

12 SPEAKER: -- real time, you know,
13 microseconds, you know, kind of sharing and, you
14 know, integrating the analysis is -- again being
15 able to do attribution. One of the great
16 questions is always well, where did this attack
17 come from? Was it the Russians? Was it the
18 Chinese? Was it this? Was it that? Was it
19 criminals? Was it -- you know -- and that's
20 probably the most difficult question to answer.
21 And the only way we're going to be able to get to
22 that is to get more of an integrated global view

1 in real time. Let me stop here (inaudible) what
2 Rich and Don have to say.

3 MR. PETHIA: Yeah, I think that's right.
4 And I do think we have information sharing
5 mechanisms in place that cause a certain amount of
6 sharing to occur. Although I think all of the
7 systems are still too careful to control what goes
8 into the common pool of information. You know,
9 again, like they use this word ecosystem. I think
10 there are things we can learn from the health --
11 World Health Organizations -- who deal with global
12 pandemics in a way a virus attack is similar to
13 that. Health organizations seem to have found a
14 way to get past this information sharing problem.
15 We knew about the H1N1 virus in Mexico and here
16 and there and someplace almost minute-by-minute,
17 while it was happening. And whatever those
18 mechanisms are, I think we need to look toward
19 some of those to find ways to get us over the hump
20 of effective information sharing because we're not
21 there yet.

22 MR. WELCH: Yeah, I would -- I would

1 just add I think that mechanism is motivation.
2 Because right now there's a motivation for private
3 companies to keep security breaches silent or --
4 and if we're going to share, we have to have the
5 proper motivations to share completely and
6 honestly and quickly. Because the reality is, in
7 most cases, we don't know if it's a security
8 incident -- especially on a network -- for quite a
9 while. Was it -- is it just a router acting up?
10 Is it -- is it a normal software bug? Is it -- is
11 it an innocent destruction of the physical
12 facilities? Or is it like we had last year in the
13 San Francisco Peninsula where it was a malicious
14 destruction of physical capabilities? That's
15 going to be really hard and the more we can share
16 information to get different views to understand
17 what's going on, the faster then we can get to
18 that -- that space. But, there's -- right now
19 that motivation is not there.

20 ADMIRAL BARNETT: Questions from the
21 audience. By the way, if you do ask a question,
22 we have a microphone and I would just ask you to

1 identify yourself. Alright, we have one -- one
2 here from the virtual world here. Craig asks and
3 I'll ask one of you to -- any of the six of you to
4 -- to jump in on this. How distributed are attack
5 sources across the world? We have control over
6 laws and consequences within the U.S.A., but not
7 internationally. If the threats are larger from
8 an international perspective, what can we do to
9 improve laws and consequences across the world?
10 Even within the U.S.A., are the laws and
11 consequences sufficient?

12 SPEAKER: Who wants to start that?

13 MR. PETHIA: Well, let me start. I've
14 certainly seen a lot of improvement over the last
15 20 years in the ability of law enforcement
16 organizations globally to work together. It was
17 the case when we started CERT in 1988 -- '89 we
18 had a lot of problems that were coming out of the
19 Netherlands and, at the time, there were no
20 computer crime laws in that country and we, you
21 know, we called up the Dutch Federal Police and
22 they said, gee, hope you find a way to solve this

1 because we can't do anything for you. But that's
2 changed. And in most of the countries today,
3 there are law enforcement organizations. There
4 are laws in place and I think we're doing a much
5 more effective job today than we were say even 10
6 years ago.

7 ADMIRAL BARNETT: Other questions?

8 Alright. Zenji.

9 MR. NAKAZAWA: Hi. Thank you very much
10 for joining us. This is really informative and
11 I'm Zenji Nakazawa with the Public Safety Homeland
12 Security Bureau, the Policy Division Deputy Chief.
13 My question is regarding the results oriented
14 approach I think is -- has its place. But
15 sometimes in a situation when you're talking about
16 such a high risk, you run the possibility where
17 when you find that result, it's often too late.
18 The attack has occurred and damage has resulted.
19 What I'm interested in is what types of
20 technologies or applications are out there to
21 actually preempt or to identify these types of
22 attacks before they actually enter the core, for

1 example, on the perimeter or near the edge. You
2 know, coming from a farming background, we used to
3 just use the shotgun to keep the dogs and things
4 away from the sheep until we realized we had to
5 tighten up the perimeter. So are there any kind
6 of early warning systems that are in play or being
7 developed that could assist in this area? Thank
8 you.

9 MR. NAGENGAST: Yeah. Let me try to
10 start the answer and then I think Don will want to
11 say something as well. As I tried to point out in
12 my talk, we do in our network- based analysis,
13 using the intelligence in our network, try to
14 detect an emerging exploit as early as possible.
15 And, you know, we do these histograms of day one,
16 day two, day three and you typically can see the
17 evolution. A zero day attack doesn't just come
18 out of the box and then start exploiting systems.
19 It takes a while. You'll see, you know, the
20 evolution of the -- of the malicious code over a
21 period of time. It might be 24 or 48 hours, but
22 they typically -- the hackers typically don't get

1 it right the first time. And so we watch the
2 evolution of the attack and then, you know,
3 depending on what the mitigation strategy is going
4 to be -- first of all, you know, we typically tell
5 our customers, hey, we're starting to see exploit
6 code against a particular vulnerability. Make
7 sure you implement the patch as rapidly as
8 possible and block -- block that attack. Or we

9 might close router ports or something -- you know,
10 do some -- again, it is very complex, but go
11 through the analysis as rapidly as we can and our
12 objective is to detect the malicious activity
13 before it's actually had a chance to do any
14 damage. So again that's not a perfect science and
15 there's always the well, this is an attack we've
16 never seen before and the first question is it
17 really an attack? Is it a misconfigured server
18 someplace that's causing the problem? So you have
19 to go through that whole -- that whole process.
20 But there are things that you can do to catch it
21 early on and that's the way we try to focus -- is
22 catch it before it does any damage. Again, that's

1 not a perfect science, but that's the approach we
2 take.

3 SPEAKER: And I'll just say for certain
4 types of attacks, we'll probably be able to do
5 that. But the vulnerability of our -- of our
6 critical infrastructures to someone who really
7 wants to do us harm and is not necessarily out
8 there playing around, so to speak, in a, you know,
9 in a hobbyist manner, is going to take a much --
10 is going to be much more difficult to do, but the
11 consequences are going to be much worse. So if we
12 had some organization that wanted to do us ill,
13 they -- we're not going to see the activity just
14 by looking at statistics. They're going to
15 collect a number of zero day exploits. They're
16 going to hit all the various manufacturers -- the
17 CISCOs and the Junipers and four and anybody else
18 who's got a router in the system -- and launch it
19 all at the same time. And they're probably going
20 to be pretty good. They're probably going to have
21 very few of them -- them fail. So how are we
22 going to -- how are we going to defend against

1 those? And, so, we need a whole combination of
2 things to defend against it. And so we need our
3 government agencies, who know what's going on out
4 there and in many ways are being offensive and
5 being proactive, to defend against those kinds of
6 things, because basically we're pretty good. You
7 know, Confiker or all these various worms that
8 come out -- they might bring us down for a couple
9 of days, which is -- which is real pain, but I
10 don't think we've seen a real serious attack on
11 the U.S. yet, and I hope we don't. But it -- but
12 the consequences would be huge.

13 SPEAKER: This is another area where I
14 think there's a place for an active research
15 program. And I agree with what I'm hearing here.
16 We're getting pretty good at detecting the things
17 we know about. We're still struggling to come to
18 understand the things we don't know about and I'm
19 suggesting -- one of the things I want to suggest
20 is maybe our approach is a little bit backwards.
21 There's a large -- almost -- it's not infinite,
22 but it's big -- number of ways that systems can be

1 attacked and bad guys are inventing new ways every
2 day. So, rather than trying to discover some
3 huge, almost uncountable, number of bad things,
4 why don't we take the opposite perspective, which
5 is within our machines, we know that there are
6 certain pieces of software and certain pieces of
7 data that should not be changed over time and be
8 able to do a better job of integrity checking the
9 systems that we have and have them check their own
10 integrity so -- they may not know exactly why
11 they're sick, but they can raise a flag and tell
12 you that they are. And that can help narrow the
13 focus of an investigation so that you can more
14 quickly discover what some of these bad things
15 are. And I think that's an active area of
16 research that would produce some fruit.

17 ADMIRAL BARNETT: Robert Cannon.

18 MR. CANNON: I want to ask a very large
19 question -- a big question. And the question is
20 is cyber security a barrier to broadband
21 deployment?

22 SPEAKER: I would say it's not right now

ANDERSON COURT REPORTING

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

1 because honestly we're probably not taking it very
2 seriously in the broadband area. And I don't mean
3 an affront to what AT&T is doing, but really
4 broadband companies -- ours included -- are in the
5 process of providing service to our -- to our
6 customers, and we want to provide robust service
7 of which security incidents are very small on the
8 service problems that we have. So, so I don't
9 think it is right now. I think if we had a proper
10 security framework and really could defend our
11 infrastructure, then we would see it be more
12 expensive and therefore that would slow down the
13 adoption. But, right now, no.

14 MR. CANNON: So, better cyber security
15 would be the barrier to deployment?

16 SPEAKER: I believe that better cyber
17 security is going to result in higher costs and
18 lower functionality. I believe that that triangle
19 that I put up there is a constant volume and it's
20 always an engineering tradeoff. So, yes, it
21 would.

22 SPEAKER: Let me just add to that.

1 Number one, you know, we believe broadband exists
2 today. I mean we're in the broadband business, so
3 it's not a new thing from a technology
4 perspective. There's no -- there's no surprise to
5 us in broadband from a technical perspective.
6 And, you know, in the enterprise space, cyber
7 security is becoming more and more of a recognized
8 requirement of doing business that quite hasn't
9 translated over into what I'll call the small
10 business consumer side of the equation. So,
11 broadband is already happening. I mean it's not
12 like well this is going to be a new technology
13 that's going to change the world. I think we're
14 talking about how do we deploy it on a broader
15 basis and get it to the places where it needs to
16 be and that's something we certainly support and
17 all the broadband suppliers support. The question
18 is how to do that and at the same time expand the
19 market awareness of cyber security so that that
20 becomes, you know, part of the whole equation. It
21 wouldn't make sense to just say we're going to
22 push out broadband and we're not going to worry

1 about security when we do that. But, you know, I
2 think we've got to work, you know, the market
3 forces and the innovation are what we need to
4 promote as we expand the broadband and make that
5 an integral part of the strategy. I don't see it
6 as an impediment, per se. I think it's an
7 opportunity and that's the way we should approach
8 it.

9 SPEAKER: And if I can contradict myself
10 for a minute --

11 SPEAKER: Of course.

12 SPEAKER: If -- if we build out more
13 broadband, we are inherently making the system
14 more secure, because the more past that we have,
15 the more capacity that we have, the more diversity
16 of systems, the more difficult it will be to bring
17 it down. But, but -- so those two things, you
18 know, the more cost we have, the less we'll build
19 out. But the more we build out, the more security
20 we'll have.

21 ADMIRAL BARNETT: Richard Hovey, please.
22 Oh, I'm sorry. Go ahead. Did you have something?

1 SPEAKER: I just wanted to say I think
2 the global society's demand for increased
3 connectivity, more communication, rapid access to
4 data -- nothing's going to stop broadband. The
5 question is not slower deployment, faster
6 deployment. The question is how do we manage the
7 security issue while we're going through that
8 deployment.

9 ADMIRAL BARNETT: Thank you. Richard
10 Hovey.

11 MR. HOVEY: I want to follow on what --
12 the build out a little bit. Are there -- we've
13 talked about a lot of the problems are coming from
14 botnets and denial of service attacks and a lot of
15 those, of course, our issue showed with Confiker
16 are infected systems. Are there problems with
17 regulations or liability concerns that make it
18 difficult for you to deal with misbehaving systems
19 in residential users homes? Or do you -- do you
20 deal with them? I mean do you -- if you see -- if
21 you see someone who is part of botnet --
22 understanding, of course, that's a worldwide

1 phenomenon, but, you know, you've got to take
2 these problems a piece at a time and the U.S. is a
3 big piece. So could you --

4 SPEAKER: I think there's a, you know,
5 right at the heart of that is a social policy
6 question. For example, you know, it's not illegal
7 to have your home computer, unbeknownst to you, to
8 be captured by a botnet.

9 SPEAKER: See now that is a legal
10 problem -- a liability problem (inaudible).

11 SPEAKER: So the reason I answered that
12 question that way is because clearly if -- if a
13 user is engaged in criminal activity, the laws --
14 the criminal laws apply. But it's not criminal
15 behavior to be capture. It can happen to any of
16 us. You know, I check my home computer regularly
17 --

18 SPEAKER: Would it be helpful --

19 SPEAKER: -- but I'm never sure, you
20 know, what's going on so.

21 SPEAKER: -- would it be helpful if
22 there are practices that says here's how you

1 identify a misbehaving, unbeknownst to the users
2 computer? Because it's two in the morning --

3 SPEAKER: Yeah, and I and think --

4 SPEAKER: -- he's sound asleep --

5 SPEAKER: Right.

6 SPEAKER: -- and, and how you notify him
7 and how you fix the problem.

8 SPEAKER: I thinks that's one of the
9 things we need to address here is what is the
10 social responsibility of the service provider to
11 tell the consumer -- and maybe that's done on an
12 opt-in basis or however, you know, structure it to
13 say, gee, your machine has been captured and --

14 SPEAKER: And do you know if you have
15 any policies for doing that?

16 SPEAKER: No.

17 SPEAKER: -- you're now the spam king of
18 Lithuania, you know, or something like that.

19 SPEAKER: I mean, there's -- I mean, in
20 that regard, of course, a lot of -- a lot of the
21 providers and I know AT&T, because I've talked to
22 their -- to their mail system people -- block port

1 25.

2 SPEAKER: Yes.

3 SPEAKER: That's a pretty standard
4 practice. And so that's kind of a, you know --

5 SPEAKER: We provide spam protection as
6 an integral part of our internet services, okay.
7 And we've got to expand that portfolio. But,
8 again, we want to make sure we do it in a way that
9 makes the consumer comfortable, that, you know,
10 that they're activities are protected, but if they
11 get infected through no fault of their own, we're
12 going to -- we're going to at least, you know, try
13 to figure out how do we notify them and help them
14 to remediate the issue if they want us to do that.

15 ADMIRAL BARNETT: We actually have a
16 question from the web on this. What mechanism --
17 this is Michelle's question -- what mechanism
18 would you think would work best to educate the
19 public about these threats and how to secure their
20 personal computers? So is there a mechanism that
21 we can use to do that?

22 SPEAKER: So let me go back to this

1 integrity- checking idea. Grandma can't maintain
2 her own computer. It's just beyond her expertise
3 and always will be. And if she has been infected
4 with software that makes her machine be part of a
5 botnet, she's probably not a terrorist, but she is
6 a disease carrier. And we have ways to deal with
7 disease carriers. We quarantine them. And we --
8 and we inoculate them from time to time. So
9 here's the business opportunity for AT&T. You
10 currently provide services like spam filtering and
11 virus filtering and what have you. How about
12 configuration management for the home user? We
13 will maintain for you a -- a pristine copy of your
14 desired operating state and if you ever get
15 infected, we'll reload for you. It's an idea that
16 I think can be developed into something that could
17 be managed over time. I think expecting home
18 users to do this on their own is just completely
19 unrealistic. There are too many tens of millions
20 of people who we would have to drag up a very
21 steep learning curve. But providing inexpensive
22 ways for service providers to provide that

1 service, I think is one path that has some hope.

2 SPEAKER: Yeah. And I think
3 fundamentally, all the carrier or service
4 providers are moving in that direction --

5 SPEAKER: Yeah.

6 SPEAKER: -- because, as you say, the
7 typical user cannot -- just cannot cope with it
8 and even if you educated them 'til -- you know,
9 for the next 20 years -- they're never going to be
10 able to cope with it. So we've got to move in
11 that direction. The question is how do we do it
12 in a socially acceptable way and education about,
13 you know, of a broad basis is absolutely necessary
14 to create the foundation to do that.

15 SPEAKER: So you're going to -- you're
16 going reduce usefulness of the computer, because
17 the home user decides they want to buy a different
18 router, they want to install some freeware or
19 whatever that right now we accept that we can
20 normally do --

21 SPEAKER: Sure.

22 SPEAKER: -- and if you have your system

1 centrally managed, you're going to lose some of
2 that utility. So there -- so I believe that most
3 of the American public will not altruistically say
4 yes, this is a problem and I'll give up some
5 usefulness to help the cause. So there's got to
6 be some motivation somehow. And if I knew what
7 that was, I'd probably be making a lot of money in
8 marketing. But since I'm a computer geek, I'm not
9 really sure how to motivate people in that way.
10 But I think that almost any step we take --
11 because we're going to have to realize, there's
12 going to be a cost with it and we've got to
13 motivate that.

14 SPEAKER: So, one other path I want to
15 suggest and that is home devices that are orders
16 of magnitude less complex than the ones we have
17 today. It's pretty easy to attack the PC I bet
18 sitting in my dining room right now, but it's a
19 whole lot harder to attack this gadget. And we
20 can learn some lessons from this class of
21 technology and apply to what's currently called
22 home computing. I think there's a lot that can be

1 done there as well.

2 SPEAKER: Good.

3 ADMIRAL BARNETT: I'd like to call on
4 Andy Ogielski.

5 MR. OGIELSKI: I would like to add a
6 comment here. I mean I think that from the
7 national perspective, we are more perhaps
8 interested in preserving ability to use broadband
9 rather than protecting citizens as a government
10 action. And when it comes to devices, there is
11 already widely deployed family of traffic
12 inspection devices that broadband providers use
13 for traffic shaping. So the five guys who
14 exchange video files do not use all the
15 bandwidths. And the guys who play games can have
16 very fast response. So we are not totally
17 unprotected and because the very same systems can
18 be used to reduce the risk to end users from other
19 types of attacks. I would be curious (inaudible)
20 what AT&T or Merit management would say to this.

21 SPEAKER: Yeah. So, I'll address that
22 first and obviously my community is much more

1 concerned about privacy than I would say the
2 average citizen is. And, so, anything that is
3 inspecting traffic looking for things that are
4 malicious is something that my community really
5 looks at with a jaundiced eye. But I -- but I
6 believe that it's not limited to the academic
7 community. So the idea of the government looking
8 at my traffic to see if its malicious, in fact,
9 would probably be a very good thing in terms of
10 securing our infrastructure. But, once again, it
11 would be a hard sell to certain sectors of our --
12 of our society. So there -- once again, we've got
13 to motivate society to change their behavior to
14 allow that -- whether it be the government or AT&T
15 or small -- small providers -- that somebody is
16 going to be looking at their traffic. That it's
17 not going to be completely private, even though
18 it's just a machine. We know that's a -- that's a
19 situation that we get to that can get out of
20 control very quickly.

21 SPEAKER: Yeah. And just to reinforce
22 that, I think when I was saying the social issue

1 around, you know, managed services gets right to
2 the heart of that. It's, you know -- I always say
3 cyber security and privacy go hand in hand and you
4 can't have one without the other, but not
5 everybody views it that way. And so anything that
6 could be inferred as now somebody -- whether it's
7 the carrier, service provider or some government
8 agency -- is now watching my behavior on the
9 internet, that gets into that -- right into the
10 heart of that social issue.

11 ADMIRAL BARNETT: Alright. Great. Yes,
12 sir.

13 SPEAKER: Good morning. I'm Rodney
14 Petersen with Educause. I want to go back to
15 Grandma's computer, because I think that speaks to
16 the heart of national broadband policy and I was
17 struck by Mr. Nagengast's comments about more user
18 education and awareness and then the last one
19 simplifying the user education -- or the user
20 experience. And I think, you know, tomorrow many
21 of you may know kicks off National Cyber Security
22 Awareness Month and there's going to be a lot of

1 efforts in schools, colleges, universities,
2 businesses across the country over the next 30
3 days for the next several days to raise awareness.
4 Given the messages that end users need versus the
5 complexity, particularly in homes that they deal
6 with -- and by complexity I'm talking about an ISP
7 that provides internet security services, a home
8 computer that comes bundled in with services, an
9 operating system that has services. The average
10 home user doesn't know how these now emerging
11 numbers of services work together or not.

12 SPEAKER: Yeah. Throw in a few service
13 packs on top of that.

14 SPEAKER: Right, right. So what are the
15 awareness messages -- and if you can again return
16 to how do these service industries work together
17 to make this user experience more simplistic for
18 the average residential broadband user?

19 SPEAKER: I think that's one of the big
20 challenges we face, is how do we integrate that
21 and simplify that user experience. The complexity
22 issue is just overwhelming today to again even the

1 typical system administrator who is trained in
2 computer science. Part of that, I think, you
3 know, there are approaches as we were talking
4 earlier about things going more in the thin client
5 direction and more hosting the applications in the
6 cloud. And I think that's going to be part of the
7 evolving infrastructure, particularly as we move
8 to 4G and LTE. I think you're going to see a lot
9 more of the sophisticated applications being
10 hosted in the cloud and not on the end device.
11 And that gives us a way -- hopefully a way forward
12 in order to be able to simplify that user
13 experience and make the cyber security thing much
14 -- much more manageable. But it's going to take
15 effort across the board between all the different
16 players in the technology business to make -- to
17 make that come together because that's not always
18 in the best interests of all the different, you
19 know, components of the marketplace, let me say
20 that.

21 ADMIRAL BARNETT: Other questions? Yes,
22 back here.

1 SPEAKER: I'm Andrew Martin. I'm the
2 CIO here at the FCC. I do have -- kind of
3 flipping back a little bit to kind of the
4 responsibility for the coordination. When we talk
5 about interoperability counsels and working groups
6 as far as sharing information, we're talking about
7 a very reactive footprint. We're reacting to an
8 item or something along those lines. But it seems
9 like you're trying to twist that towards a more
10 proactive footprint. However, what is -- where is
11 the organization -- how do you manage that, that
12 proactive view towards dealing with the cyber
13 security issue? So anywhere from education from
14 the simplification standpoint towards getting all
15 the players across the board to talk beforehand,
16 make sure that they're products are doing what
17 they're supposed to be doing and have gone through
18 the rigorous tests. I know there's research and
19 development on the table, but I know a lot of
20 interest there, and it would be easier if we could
21 capture that stuff upfront prior to reacting to it
22 when it comes through on the other end with an

1 incident or not.

2 SPEAKER: Want to try that one, Rich?

3 ADMIRAL BARNETT: They're prompting each
4 other. You answer that one. You answer that one.

5 SPEAKER: That one's hard. You have it.

6 SPEAKER: So -- so I think being
7 proactive is going to be the absolute -- the
8 absolute key. So if we think of this cyber space
9 is a battle field, which it essentially is.
10 You've got people trying to do bad things to good
11 people. Then if we're always on the defensive,
12 we're always reactive, we're going to lose. So we
13 need to be proactive. And, of course, the
14 question on proactivity then you really have to be
15 careful about legal bounds and especially as it
16 goes across countries and so forth. You know,
17 what can we do? Because if we sit there and wait,
18 bad -- bad guys -- you know, whoever they may be
19 and whatever their motivation is -- they can focus
20 both their resources and in a timewise on a very
21 small area that, you know, we just can't afford --
22 can't afford to match and the only way really to

1 defend against it is to unplug everything. So
2 we've got to find that right balance. And in my
3 mind, the -- there's a role for the federal
4 government, much as there is in the common
5 national defense, for the defense of our systems.
6 Now it's going to be a little different than --
7 than the physical defense, but I think the role is
8 still there. And exactly what it is is going to
9 be difficult to define, but it -- but it is
10 something. So there's some coordination. There's
11 some -- there is some motivation. There's that.
12 But this whole idea of a defense in depth probably
13 needs some kind of a central controlling agency.
14 I don't have time to go into my thoughts on it
15 completely, but I think there is a strong role for
16 the government, whether it be in DHS or the FCC.
17 Of course, the way the government works, it's
18 going to be in a million different places. But
19 really, where somebody puts it together and helps
20 set a guideline and a policy and sets the right
21 balance.

22 ADMIRAL BARNETT: Okay. Did I see

1 another question over here? Yes, sir.

2 MR. PEERY: Hi. I'm Ashton Peery with
3 Renesys Corporation. Question about economics and
4 policy and the interplay between the two. In a
5 world where we hear today there are carriers
6 globally that are pricing broadband at less than
7 \$2 a megabit, when it used to be a year or two ago
8 maybe \$60 a megabit -- the economics are such that
9 I don't -- I can't understand how any service
10 provider could afford to implement the kind of
11 security that we would like to see. So the
12 question is, under those circumstances, would
13 industry appreciate and prefer to have some
14 government mandates to help push security forward
15 in a way in which that cost is shared and borne by
16 all as opposed to those who might try and use it
17 as a competitive advantage?

18 SPEAKER: Well, I think the interesting
19 part of that question is, you know, what would you
20 mandate if there were government mandates? As we
21 were talking earlier, it's a very dynamic problem.
22 And, you know, just when you think you understand

1 at least the problem, it changes on you and you
2 don't even have -- developed the answer for
3 yesterday's problem yet. So the whole issue with
4 mandates and, you know, trying to regulate in --
5 if I want to use that word -- regulate in
6 security, is how do you even define what the, you
7 know -- I like the, you know, we're going to look
8 for results. We're reminded back to the old
9 Ghostbusters movie where the guy says well, you
10 know, in the private sector we demand results, you
11 know. But, you know, what is that result? How do
12 you define that? What are the metrics you're
13 going to use to achieve success? And I've had a
14 lot of experience in my government days with
15 certification programs like the NIAP -- the
16 National Information Assurance Partnership -- with
17 NISC that did the -- that does the certification
18 against the common criteria levels. And they
19 typically tend to stifle innovation because you're
20 always certifying, you know, the last generation
21 of product through the process. So, you know, as
22 we think about how do we motivate it? You know,

1 first of all, I absolutely believe it's got to be
2 driven by market demand. I think industry
3 responds best to market demand. When the
4 consumers, customers say this is what -- I want
5 cyber security. They're going to get cyber
6 security one way or another, okay, and we'll have
7 to work our way through that. Trying to direct
8 dictate that is very, very difficult because it's
9 one of these be careful what you ask for, you're
10 not quite sure what you're going to get. Because
11 we really haven't been able to define meaningful
12 security metrics in any -- in any precise way and
13 that's part of this challenge here. If we could
14 measure it, then we could -- maybe we could figure
15 out how we can shape it. But first we got to
16 figure out how to measure it.

17 ADMIRAL BARNETT: Others on that? Well,
18 so -- a follow up question -- we've had one
19 question from Cynthia that talks about application
20 security checklists and my own question about the
21 certification process. So would you say then that
22 the FCC should consider or not consider a

1 certification program -- considering that there
2 were some type of cyber security standards set up
3 or best practices where they were, you know, you
4 could certified in this by a -- communications
5 providers could get certified.

6 SPEAKER: Well, my quick answer and then
7 I'll let others talk is, you know, certification
8 might be a useful thing if you can define what it
9 is you're certifying. Again, in a way that's not
10 going to stifle the innovation that's required and
11 keep up with the dynamics and the technology.

12 ADMIRAL BARNETT: Right.

13 SPEAKER: One of the reasons the attacks
14 are changing every day is because the technology
15 is changing every day. So when you think about,
16 you know, what is this end result that I'm going
17 to try to achieve and it's easy to say, you know,
18 more security, but defining that in a meaningful
19 way and then trying to figure out how would I
20 certify that without stifling innovation and if
21 I'm certifying, you know, last year's product
22 when, you know, we've moved two generations ahead,

1 that's not going to be particularly useful. I've
2 been there and done that and it doesn't really get
3 you where you need to be.

4 SPEAKER: So I would say absolutely not.
5 And I think it might be theoretically a good idea,
6 but in a practical sense, I would see it'd be
7 almost impossible to implement well. The -- you
8 know -- and I say if we look at DOD and how they
9 are struggling to do that and the arguments that
10 go on over innovative use of technology, the
11 ability of the war fighter to conduct their
12 mission and so forth versus the security, as I say
13 and that's a homogenous type of a -- type of a
14 problem. So I think it would be almost impossible
15 for a single agency to mandate these are the best
16 practices, these are the checklists, these are the
17 kinds of things that we need to do and keep
18 innovation and keep the economy growing and
19 actually not do a denial service attack on
20 ourselves. So I think the -- as I said -- if we
21 could in some way incent the marketplace to
22 provide more secure products, that would be the

1 key. And I think we will get the fastest results
2 and the best results if we do that. And I would
3 say that, you know, there is some way of mandating
4 or holding people accountable for results that
5 could be worked out that would be much more
6 effective than trying to say these are the best
7 practices. If you don't follow them, you're on
8 your own.

9 ADMIRAL BARNETT: Okay. Alright.
10 Richard Hovey?

11 MR. HOVEY: I want to pick up on
12 something that Richard Pethia said which was --
13 talked about sort of organizational resiliency and
14 so I think the notion there might be that an
15 organization has a security culture that you can
16 depend on that in turn would dictate that they
17 apply the best practices, without you -- because
18 it's going to be different best practices for
19 every organization. And so I guess my question
20 for Richard is first, does that -- do those
21 schematics apply equally? I mean they seem to be
22 maybe organized more towards the enterprise

1 customer, but would they -- they would probably
2 apply to a service provider. And then secondly,
3 although something against which one could
4 reasonably audit the security culture, you know,
5 such as the training components, the decision
6 making components when faced with having to make a
7 decision and so on. I mean you had quite a list
8 there. Could you maybe address that?

9 MR. PETHIA: I was okay until you got to
10 the audit piece.

11 SPEAKER: Well, that was the question.
12 I mean --

13 MR. PETHIA: The models I think are
14 available. They're available from us. They're
15 available from a lot of places. Certainly the
16 people who are active in the area of risk
17 management are going to keep pushing those models
18 and ideas forward. I think they're pretty well
19 evolved now. They're going to continue. The
20 profile that any particular organization needs
21 with respect to all those practices -- this is
22 going to vary from organization to organization.

1 So trying to having one yard stick that fits all
2 organizations, I don't think is a meaningful thing
3 to do. I also think the audit would be an order
4 of magnitude at least more complex than any of the
5 typical audits that I see being done by standards
6 organizations or government organizations today.
7 Looking -- looking at a set of controls and
8 identifying whether or not they're in place is one
9 thing. Looking at a dynamic set of processes that
10 need to change over time and adapt to changing
11 risk and threat profiles is something else again.
12 And I think it takes a very special set of
13 auditors to be able to do that. So, I'm very
14 concerned about propagating the idea that a simple
15 set of controls solves the problem and, with our
16 experience of having some pretty simple-minded
17 audits go on, I don't know that we get the benefit
18 that we want from that investment.

19 SPEAKER: Yeah. My only comment there
20 is when you think about audit, think FISMA as, you
21 know, a process that was very, very, you know,
22 intensive and costly and didn't result in a whole

1 lot of increased insecurity across the government
2 agencies all go through the FISMA compliance
3 process.

4 ADMIRAL BARNETT: Alright. John?

5 SPEAKER: I want to follow up on a
6 comment of Don Welch. If I understand right,
7 you're suggesting we mandate results and part of
8 mandating results is requiring disclosure --

9 MR. WELCH: Right.

10 SPEAKER: -- of security issues or
11 problems. Now there's a long history in the
12 telephone world where we mandate, either to the
13 regulator or the public, disclosure of outages, but
14 I know what an outage looks like. I know how to
15 measure it in number of telephones --

16 MR. WELCH: Right.

17 SPEAKER: -- or duration. So I want to
18 first, for the whole panel, is it a good idea to
19 require some kind of disclosure? And, if so, how
20 do we figure out what it is you should be trying
21 to report?

22 MR. WELCH: Yeah. So, so I did caveat

1 my remarks by saying this would be hard. So I
2 think you're absolutely right determining what a
3 security incident is and whether it's reportable.
4 So in the abstract sense, you know, I think it'd
5 be good. It would be a lot of work, but I think
6 it's the way that we could drive market forces if
7 we had a system for disclosure and that gets us
8 also along the lines of sharing and a more of
9 shared understanding of what's going on and
10 getting a bigger picture. Because right now,
11 there are negative incentives to disclosure.

12 SPEAKER: Can I just follow up on and
13 maybe a question for John is I suspect that
14 internally ISPs have definitions as to what
15 constitutes an outage that they -- when they feel
16 it's necessary that this reaches a certain
17 threshold that we have to tell our customers or we
18 have to tell our CEO, so I have a feeling that the
19 problem probably has been addressed internally --
20 maybe in different ways, but by the service
21 providers. They must have a way of classifying
22 what constitutes a major outage. They've lost

1 50,000 DSL users. We better tell somebody that --
2 you know -- or we better put something up on the
3 website.

4 SPEAKER: Yeah. And that's literally
5 true. I mean we have a process -- an alerting --
6 we call it an alerting process, which again -- you
7 know again, the first question is well what's a
8 cyber event? Well, you know, a cyber even -- we
9 see, you know, cyber events as every packet, you
10 know, that comes inside -- coming through that's
11 bad. So, but, you know, we're always in the mode
12 of watching, you know, something that might effect
13 our capability to deliver services to the customer
14 base. And that, of course, is our first threshold
15 to say, okay, you know, this has gone beyond
16 business as normal. You know, we see malicious
17 code churning through the network all the time.
18 And so when we see something that's actually has
19 the potential to interrupt service, that's when we
20 go into the second stage of the process, say hey,
21 we got to deal with this. This is not just the
22 everyday -- an everyday event. And we work our

1 way through -- up through the hierarchy there.
2 But again it's a very complex process. We've seen
3 attacks against enterprise DNS servers that
4 happened to be attached to our network by an
5 enterprise customer that started choking the
6 channels with bogus DNS queries. So again that's
7 one example of the complexity that we're dealing
8 with. That was an -- that was an actionable event
9 and it turned out what we needed to do in that
10 case was get in touch with the customers who had
11 misconfigured their DNS servers and get them to --
12 get them to fix it. But they were starting to
13 saturate our DNS proxies with bogus, you know, DNS
14 queries that were being reflected through these
15 enterprise -- misconfigured enterprise DNS
16 servers. So, again that's one day in May that we
17 saw that -- that all happening and quickly went
18 into the get in touch with the customers. We
19 quickly identified where were these rogue DNS
20 servers and dealt with it. But, again, that's --
21 now is that something we needed to report to
22 management? Well, we did up through our normal

1 management process.

2 SPEAKER: Should you have then -- along
3 Don's comments been -- then reported that incident
4 outside of management? Should it have come to --
5 I don't know -- a government agency or perhaps --

6 MR. PETHIA: Well, we deal with U.S.
7 CERT. For example, U.S. CERT is one of the points
8 we would report an incident like that to. And we
9 go through -- there's a kind of dual reporting
10 chain through the NCC -- the National Coordinating
11 Center and the U.S. CERT, which are collocated at
12 DHS now and that's the first place in government
13 we would -- we would call and, you know, tell them
14 gee, we've just seen this particular kind of event
15 taking place in our infrastructure and then they
16 would be -- you know -- might -- Verizon might
17 make the same call, you know, the next day or
18 whatever, so. So that's kind of the process we go
19 through today. But clearly the first thing that
20 matters to us is when we go from, you know, this
21 is business as usual and the usual cyber events to
22 hey, here's something that has the potential to

1 interrupt service to our customers and that's when
2 we go into the next level of intensity.

3 SPEAKER: And especially in a small or
4 medium sized ISP, your first priority is to
5 restore service and then your second priority is
6 to try and understand what the problem was. And
7 so as a result, if it was malicious code, in many
8 cases you'll destroy the evidence in restoring
9 service and you'll never be able to figure it out
10 or you'll never have the time to get to the bottom
11 of it because it's -- it takes a lot of time and
12 complexity to figure out exactly what went on.
13 But service is working again and you've got a long
14 to do list to do. So right now the motivation is
15 not to in any ways -- to make sure that you
16 understand what goes on in terms of a malicious
17 activity or then to report it anywhere. There
18 isn't a -- there isn't a real incentive to do
19 that. And that I think is part of the issue and
20 as I think the gentleman from Renesys said, you
21 know, the profit margins in the -- in the ISP and
22 the carrier (inaudible) are very, very small and

1 people perceive bandwidth as a commodity and they
2 think up I should turn on the light switch and
3 just like, you know, electricity it should be
4 there and bits are bits and they don't necessarily
5 want to pay more for something that -- for higher
6 quality that may include security. So it really
7 does make it hard in the day-to-day operations and
8 changing the incentive structure I think is the
9 only way that's going to -- that's going to
10 change.

11 ADMIRAL BARNETT: Do you have a question
12 over here?

13 SPEAKER: Robert Mayer, U.S. Helicopter
14 Association. I think we're about -- almost to the
15 anniversary of the Confiker worm a year and you
16 had mentioned that we were still uncertain about
17 its origins I think and what its purposes are.
18 And I'm wondering if we could use that as a real
19 -- a real life example of a current threat, an
20 evolving threat in terms of sophistication and
21 impact and how you would relate that kind of
22 example to the notion of best practices or

1 standards or certification. What would be done in
2 that area that would change how we're currently
3 responding to -- or would have responded to the
4 Confiker worm -- especially in light of the fact
5 that it's almost a year. We're in multiple
6 variance right now and it seems there's still a
7 lot of uncertainty about that.

8 SPEAKER: Where do you want to start?
9 Okay, let me take the first shot at that question.
10 I think that's a great question. You know, what
11 I'll say is right now because it's out there, and
12 we haven't been able to mitigate it, it's still on
13 millions of machines, I mean that kind of points
14 to the, you know, kind of one of the hearts of the
15 problem is, okay, you know it's there, but what
16 are you going to do about and how do you mitigate
17 that? So, you know, there is no best practice
18 with respect to Confiker today. It's -- even if
19 you know you've been infected, the next challenge
20 -- okay, I've been infected. Now what? And, you
21 know, at that point in time, you might as well
22 just unplug your machine and throw it -- you

ANDERSON COURT REPORTING
706 Duke Street, Suite 100

Alexandria, VA 22314
Phone (703) 519-7180 Fax (703) 519-7190

1 know -- throw in the trash bin and start over and
2 hope you don't get -- hope you don't get hit
3 again. But, but -- so that's an example of some
4 of the complexities involved with dealing with
5 something that is in -- and again it continually
6 gotten more sophisticated and more difficult to --
7 to deal with as far as mitigation even if you know
8 it's there. And again, we track it, so we know
9 where it is and we know it's -- all over the
10 world. It's a global threat. And even in the
11 U.S., we haven't been able to mitigate the
12 challenge there. And, you know, I'm not sure where
13 else you'd want to take that other than clearly
14 that's something that the industry needs to come
15 together and do a better job on in terms of how do
16 we mitigate these kinds of threats -- and it's
17 across the whole infrastructure.

18 ADMIRAL BARNETT: From the web, Brian
19 asks a follow-up question to Dr. Welch. Dr. Welch
20 said filtering customer traffic based on whether
21 it's malicious or not would be a hard sell for
22 customers. Well what about filtering based on the

1 destination? Many of today's threats are at
2 websites or networks that have a very bad
3 reputation and have had that reputation for some
4 time.

5 MR. WELCH: Yeah. Most -- it's fairly
6 trivial. In fact, I used to teach it in a class
7 on information security to nontechnical students
8 to route your attacks around different --
9 different computers and use different hosts to
10 jump around. So, identifying where a threat comes
11 from is really very hard -- to be able to block it
12 at its original source. It's extremely easy to
13 get -- to get around those kind of -- those kinds
14 of blocks.

15 ADMIRAL BARNETT: Okay. Yes, Robert?

16 SPEAKER: A number of times in this
17 conversation, we've discussed education as one of
18 the solutions for cyber security and I want to
19 contrast this to a different panel we've had which
20 is on-line safety -- very similar but different --
21 dealing with children and offensive content.
22 Could you talk a bit -- it's a two part question.

1 What about your outreach efforts? In on-line
2 safety, the big term is media literacy, working
3 with the kids, working with the schools and the
4 teachers, teaching them how to use these tools.
5 Can you talk about educational efforts and their
6 effectiveness? And then, in particular, I know
7 that a lot of the ISPs give the safety and
8 security software for free or as a part of their
9 installation package. Do you have any sense of
10 how much the users are using these packages and is
11 that a part of the education? They are getting
12 educated and then they're using these packages.

13 SPEAKER: Yeah. Well, I think, you
14 know, we're very involved in a lot of the
15 educational efforts that are going on today --
16 both at the, you know -- both at the beginning of
17 life when you're in -- when you're in elementary
18 school and at the later stages with the -- you
19 know, with the older population -- and I'm getting
20 there very rapidly. But, you know, education can
21 only go so far and, you know, making the users
22 aware of the concerns -- I mean you start with the

1 basics like if you get an email saying you've just
2 won the Ugandan lottery, and you've never entered
3 the Ugandan lottery and all you've got to do to
4 collect your money is send your social security
5 number and your bank account to us. If you
6 respond to that, that's probably not a bad idea
7 and that, of course, is part of what the process
8 is all about. But then when you get into the
9 sophistication of dealing with it on a daily basis
10 -- and it's easy to put in some -- there are some
11 things you can do and blocking bad websites and
12 parental controls and things like that. But once
13 you get beyond that and you get an icon that pops
14 up on your screen that says your system has just
15 been compromised and then to save yourself, click
16 here and we'll take care of you. You know, how do
17 you deal with that? And, you know, is it legit or
18 is not legit? And, you know, both. I mean I get
19 these pop-ups on my computer all the time saying
20 Microsoft has a new patch for me. My first
21 question is well how do I know it's really
22 Microsoft that wants to download this patch onto

1 my machine. My friends at Microsoft tell me I
2 don't have to worry about that, but that icon can
3 be trusted. But I'm not so sure about that. So
4 that's part of what -- you know -- getting -- you
5 know -- making people aware is absolutely
6 important and -- you know -- you start with that
7 first line of defense. But when you get into the
8 sophistication of the ways that the criminal mind
9 has created to fool even the most well-educated
10 and wary consumer, you know, it's very difficult.
11 And that's where I think we got to get out of the
12 -- you know, we can't educate the consumer to the
13 point where they're going to be able to deal with
14 this -- with this issue. We've got to be able to
15 help them, you know, in providing demanded
16 security services, you know, that are going to be
17 necessary to deal with this on a broader basis.

18 SPEAKER: Part of the educational
19 message is is virus protection --

20 SPEAKER: Right. Absolutely.

21 SPEAKER: -- update or operating
22 sufficiently? Are people responding to that, and

1 is that -- because that's part of the complexity
2 of getting hit by something you don't know.

3 MR. WELCH: Let me give an example on
4 that and how we work against ourselves. So a
5 computer vendor, to remain nameless, just got a
6 very good marketing program. I was at a friend's
7 house. They bring home the new computer for their
8 daughter and oh, we saved a bunch on money because
9 these computers don't get viruses, so we didn't
10 have to buy antivirus software and then oh, can
11 you help me hookup to our, you know, unsecured
12 wireless network. We can't get it to work. And
13 this is a very educated family. So, it's a steep
14 curve that we'll have to climb to get there.

15 ADMIRAL BARNETT: So, as it turns out, I
16 think Dr. Welch gets the last word on this. I'd
17 like to thank each of you for being here. For all
18 the people that -- who attended via the web --
19 including questions that we got from Cynthia,
20 Brian, Michelle, Craig, Eric, Prudence and Jeremy.
21 We have those questions and we're going to
22 incorporate those. I'm sorry we didn't have time

1 to get to all the questions there or here. And
2 then a special word of thanks -- number one, I'd
3 like to thank the folks who helped set this up. A
4 lot of work went into this and then for our
5 panelists up here, I think we all owe a debt of
6 gratitude. Thank you very much, particularly our
7 guests, for being here. Jennifer, at this point,
8 I'll turn it back over to you.

9 MS. MANNER: Thank you very much and
10 thank you for our panelists. We're going to take
11 a 15 minute break. So I would ask that everyone
12 please return to the conference room at 10:45 for
13 our second panel. Thank you and thank you very
14 much.

15 (Recess)

16 MS. MANNER: -- the second panel of the
17 Cyber Security and Broadband Workshop and I'm
18 going to turn the floor over to Jeff Goldthorp,
19 who is Chief of the Communications Systems
20 Analysis Division in the Public Safety Homeland
21 Security Bureau, who is going to moderate this
22 panel. And thank you.

1 MR. GOLDTHORP: Thank you, Jennifer.
2 And welcome back everybody. I'm looking forward
3 to our second panel and welcome our panelists and
4 also our FCC panel. Let me first start by
5 introducing the FCC panelists very quickly and
6 then I'll go through the other panelists in more
7 detail. First, starting at my -- at my left is
8 Jean Ann Collins. Jean Ann is Deputy Chief of the
9 Communications Systems Analysis Division here at
10 the Commission. Next to her is Bob Cannon. You
11 met Bob on the first panel. He's the -- he's the
12 Internet Law Advisor -- Senior Internet Law
13 Advisor here at the Commission. Next to Bob is
14 Rich Hovey and you met Rich on the first panel as
15 well. He's -- he's a Telecom Systems Analysis
16 here at the Commission. And then finally Jon
17 Peha, also on the first panel, and he's Chief
18 Technology Officer here at the FCC. Now, moving
19 on to our panel -- our second panel this
20 afternoon, we have five panelists for this panel
21 and I'm going to start -- seated next to me is
22 Marc Donner. Marc is Engineering Director of

1 Google Health, Google Finance, AdWords
2 Engineering. Dr. Donner has over 30 years of
3 experience in engineering of hardware, software
4 and complex systems. Before joining Google Health
5 and Finance, Dr. Donner was the Engineering Site
6 Director for Ads Development in New York and
7 oversaw the integration of dougle clicks -- double
8 clicks rather engineering teams and technical
9 products into Google. Dr. Donner previously
10 worked at Morgan Stanley as an Executive Director,
11 IBM Research as a Researcher and at NASA's Jet
12 Propulsion Lab. Dr. Donner also serves as
13 Associate Editor in Chief of the IEEE Computer
14 Society Magazine, Security and Privacy. Next to
15 Dr. Donner, but actually not quite -- virtually
16 next to Dr. Donner, joining us on the -- on the
17 video conference -- there we go. We were actually
18 having a little bit of trouble of that this
19 morning. Ironically we had the video working
20 great, so the broadband was cooking good, but the
21 -- but the telecom was sort of not cooking so
22 good. But, that's been fixed since so -- welcome

1 Allan. We're glad to have you on board. Allan is
2 the IT Director, North Carolina State Highway
3 Patrol, where he's responsible for managing and
4 supporting a 140 site network to support law
5 enforcement personnel in North Carolina. He also
6 serves as the IT Security Lead for the North
7 Carolina Department of Crime Control and Public
8 Safety as well as the Voice Interoperability
9 Program for Emergency Responders. He's a retired
10 United States Air Force Major, whose
11 accomplishments include U.S. Air Force
12 Intelligence Officer of the Year and originator of
13 the Department of Defense Standard Secondary Image
14 Disseminator System. Next to Allan -- excuse my
15 fumbling around, but -- is Dale Drew. Welcome,
16 Dale. Dale is Vice President for a Security at
17 Level 3 and he's got over 21 years of professional
18 security experience working in law enforcement and
19 global ISP security capacities. He's designed,
20 built and deployed security infrastructure and
21 threat analysis tools used to monitor and protect
22 company assets in global networks. He's also

1 built world-class security departments from the
2 bottom up. He's worked in designing, developing
3 and deploying commercial security products for
4 over six years and he's worked on professional
5 computer forensic capabilities for 16. Mr. Drew's
6 experience is focused on protecting some of the
7 world's largest public network environments. Next
8 to Dale is Andy, Dr. Andy Ogielski. He's
9 President of Renesys Corporation. Dr. Ogielski
10 has more than 30 years of experience encompassing
11 data networking, internet architectures, wireless
12 networks, software systems and scientific
13 computing. In 1999, he cofounded Renesys and
14 Renesys is a company specializing in internet data
15 analysis and generation of mission-critical
16 real-time information on the state of the global
17 internet for network service providers, internet
18 enterprises and cyber security organizations.
19 Prior to founding Renesys, Dr. Ogielski was a
20 Professor at Rutgers University, where he led
21 government-funded research on scalable internet
22 modeling that enabled detailed analysis of attacks

1 on very large networks. And then finally -- and
2 I've got to search for this one because I don't
3 have it right in front of me -- we have Phil
4 Reitingger. Phil is Deputy Undersecretary of the
5 National Protection and Programs Directorate at
6 the Department of Homeland Security. Mr.
7 Reitingger's current responsibilities as Deputy
8 Undersecretary for National Protection and
9 Programs Directorate includes overseeing the
10 protection of U.S. government computing systems
11 from domestic and foreign threats. He previously
12 served as Chief Trustworthy Infrastructure
13 Strategist at Microsoft Corporation, where he was
14 responsible for helping improve the protection and
15 security of the critical information technologies
16 infrastructure. Mr. Reitingger also serves as a
17 member of FEMA's National Advisory Counsel where
18 he advises FEMA -- the FEMA Administrator -- on
19 aspects of cyber security related to emergency
20 management. He was previously the Executive
21 Director of the Department of Defense's Cyber
22 Crime Center charged with providing electronic

1 forensic services and supporting department-wide
2 cyber investigative functions. Before joining
3 DOD, Phil served as the Department -- rather the
4 Deputy Chief of the Computer Crime and

5 Intellectual Property Division at the U.S.
6 Department of Justice. So welcome all of you --
7 very distinguished biographies, all of you. Let
8 me now turn it over to Mr. Donner -- Dr. Donner,
9 from Google -- and ask you if you would share with
10 you some opening remarks.

11 DR. DONNER: Thank you very much. So
12 one of the -- one of the things they taught me in
13 Security 101, which they didn't have back when I
14 was young and learning the stuff, was that the
15 first secret in dealing with a security situation
16 is to understand the threat and then plan your
17 mitigations accordingly. So in order to explain
18 what it is that we're thinking about here at
19 Google in some of these areas, I'll sort of
20 describe the two threats that are -- that are most
21 -- uppermost in our minds right now. One is the
22 -- the industrial scale harvesting of -- of

1 credentials that's used for theft -- identity
2 theft that has become sort of a major focus of
3 people's attention. This is accomplished across
4 the internet by means of key loggers, compromised
5 websites, phishing and cracking into corporate
6 databases and stealing large quantities of
7 information from them. So there's a tremendous
8 amount of stuff that goes on in that space.
9 That's one -- one of the threats. The other big
10 threat is the -- the continued growth of botnets,
11 large collections of zombie computers infested
12 with malware that allows the controller of the
13 botnet to direct the machines to act in concert --
14 either widely used for denial of service attacks,
15 generation of spam and a variety of other sort of
16 malign activities. One -- and a thing that's very
17 interesting about these botnets is that they're --
18 they have migrated from toys of sort of -- of
19 cowboy bad guys, if you like, to the tools of a
20 professional criminal class and possibly used by
21 terrorists and potentially even national actors.
22 The attack that many of you will remember over a

1 year ago on Estonia during the midst of a big
2 dispute over the location of an old statue was an
3 example of that. It was one of those cases where
4 there was never any evidence of national action
5 and, in fact, analysis shows that the cost of the
6 attack on Estonia that essentially shut down its
7 banking system and a lot of governmental services
8 and a collection of emergency services -- that
9 attack probably cost no more than \$100 dollars to
10 mount. Why do these things concern us? One of
11 the big reasons is that if as a -- as a world, as
12 a society at large we don't address these kinds of
13 vulnerabilities of the internet as a whole, the
14 viability of the -- of sort of the digital economy
15 is at risk. After a while, people will say well,
16 you know, if I can't operate my fire department
17 and my police department, my other first
18 responders -- my hospitals, weather service --
19 whatever over the internet because it may be
20 attacked by these bad guys, then maybe I won't use
21 the internet that way. And that's, you know, a
22 big concern if you depend on the internet for your

1 -- for your business. So what kinds of things can
2 you do to mitigate these -- these kinds of things?
3 We've done some things. There's a lot more to be
4 done. One of the things we discovered over time
5 was that as -- as the spider at Google.com
6 traversed the internet, we could tell compromised
7 websites. And so what we've begun to do is --
8 well, we -- well, we have sort of implemented some
9 time now is if you try to navigate to a
10 compromised website, we will warn you with a
11 little pop-up that says basically if you -- if you
12 go through to this website, there's a good chance
13 that -- that something bad will happen to you.
14 It's a bad neighborhood. Don't go through there.
15 We won't stop you from going there, but we will,
16 in fact, warn you that we've detected compromise
17 on that -- on that website. We sponsor an
18 organization called Stopbadware.org., recognizing
19 that -- that all of this stuff is a community
20 effort on a very large scale and that we all
21 benefit from doing that. So we give them money
22 and a variety of support. One of the things to

1 think about that I think is necessary in
2 situations like the attack on Estonia or the
3 recent attacks on Georgia, you can say well, cui
4 bono, who's the -- who's the likely national
5 actor? But in the absence of proof of a national
6 actor, you can't really act. But what you can do
7 is you know who the victim is and you can, in
8 fact, begin to say how could I help the victim?
9 It's -- it is the case that a variety of people
10 went to help Estonia during the attack on it. Is
11 there anything that we should or could do to make
12 those kinds of responses more efficient and more
13 effective going forward? And finally, the thing
14 to think about and -- you know, Google is not an
15 ISP, so we can't actually do this, but you could
16 easily instrument the -- you could easily
17 instrument the end point routers and enlarge ISP
18 to delicately sample the session initiations and
19 accumulate those in a -- in a monitoring station
20 somewhere and then look at the statistics of that
21 and you'd see that when a -- when an attack is
22 underway, you'd actually see a spike in the

1 activity targeted at that website. You might also
2 be able to detect the activity of the -- of the
3 zombies calling home to the -- to the controlling
4 site. So there's a lot of interesting things that
5 could be done out of that. These are just some of
6 the basic ideas. Thank you very much.

7 MR. GOLDTHORP: Thank you, Dr. Donner.
8 Before we turn to Allan for some remarks, let me
9 ask I just want to ask -- to remind all the
10 speakers to just put your mic just a little bit
11 closer because they're placed back I think a
12 little bit at the start. Okay. So, let me turn
13 now to Allan Sadowski, who is joining us on the
14 video bridge.

15 MR. SADOWSKI: I certainly hope this
16 will work. I did a prepared presentation -- Power
17 Point -- so I hope you all can see it. Can you?

18 MR. GOLDTHORP: Yes.

19 MR. SADOWSKI: Okay. So this is just
20 one public safety perspective and I have a
21 standard disclosure statement. I have to do it,
22 being in the legal community. And a little bit

1 about what I'm going to do today. And primarily,
2 I'm going to talk a little bit about from the
3 perspective of being a consumer, because we will
4 always be attacked and so nothing shy of a total
5 shut down would actually protect us. So all our
6 efforts -- although good -- they will never end.
7 The public safety mission -- what IT is not the
8 primary mission. Ours is obviously first response
9 for public safety and what's important for me to
10 point out is that public safety -- the law
11 enforcement, fire, EMS -- responds in rural,
12 tribal, wilderness, marine and park areas. It's
13 not just in cities and towns. And that even with
14 no information technology capability at all -- no
15 broadband, no infrastructure -- public safety is
16 still going to respond albeit with some reduced
17 capability. The fifth slide -- the broadband
18 security protection. Today, I can say, as the IT
19 manager, I get little information from the
20 providers, but I'm not faulting them. They look
21 probably to us and say, well, IT security is not
22 the primary focus of public safety and it's not.

1 How many of the agencies have staff that are
2 dedicated to the issue? How many law enforcement,
3 in particular, have staff working cyber security
4 vice cyber crime? And then of the 45,000 plus
5 public safety agencies, how many of them need to
6 focus on the issue? How -- you know -- that'd be
7 a lot of redundant efforts and as the previous
8 panel, I'd say the ROI and that would be pretty
9 bad. On the sixth slide, it's important for me
10 that to remind everybody that for much of public
11 safety we are in the field. We're not in our
12 offices when we're actually doing our job. And so
13 mobile broadband -- I haven't heard much about it,
14 but it's -- if broadband is going to be useful for
15 public safety, mobile broadband is going to have
16 to be a component of that. And it needs to be
17 secure and with the redundant links -- with
18 systems backed up so that it can support the
19 public safety first personnel -- the first
20 responders in the field. And I have to say that
21 today -- I mean there was a point made earlier
22 about that broadband is not a new technology.

1 Well, that may be fine in urban areas, suburban
2 areas and fixed locations. But for first
3 responders, most of them have no mobile data --
4 mobile access. That includes locals, state,
5 tribal and -- at least in my experience -- quite a
6 number of federal first responders as well. In
7 broadband security protection -- and I look at IT
8 as systems and networks -- although some agencies
9 are large enough to support IT security, most rely
10 on outside agencies, have limited capability at
11 all and a few maintain any organic broadband
12 capabilities themselves. My agency is a little
13 bit different. We do some ourselves because we
14 can operate -- we can sever ourselves from the
15 internet and still work with our partners
16 internally, but it's again at a reduced capacity.
17 Why don't some agencies have broadband and
18 broadband security support? Well, it comes down
19 to awareness and resources. That should be no
20 mystery. On the eighth slide, some of the issues
21 are the provisioning of those redundant links.
22 These may be obvious for most people here, but

1 remember in public safety, IT and broadband is not
2 the number one role as a part of the mission.
3 It's a support function. And to support IT
4 security and broadband security and broadband
5 links requires additional resources. No mystery
6 there. Small agencies have few resources to draw
7 upon and there's a culture by and large that I've
8 heard over and over again within public safety is
9 that if we don't own it, then we can't control it
10 and it can't be relied upon. The common response
11 well, we can give you a great service level
12 agreement to address to that, but that adds to the
13 resource burn. So it's a circle there. I did
14 hear some comments about training -- next slide.
15 Certainly effective state of the art training is
16 important. It must be exercised and tested if --
17 to be effective. Regularly tested, which is
18 problematic because many might understand --
19 security testing for -- is sensitive and could be
20 embarrassing, frankly. But -- so it should be
21 widely disseminated. But you might be advertising
22 some of your weaknesses, but to have sanitized

1 results might be useful and full scale testing of
2 operational systems obviously can only be
3 performed if backup systems are operating. The
4 day-to-day mission cannot be impacted. It's
5 safety of lives and we take it seriously. Slide
6 10 -- the need -- integrated public safety
7 security broadband. We need it. And we need it
8 in the field with mobile and I think -- I hope a
9 lot of the people here will go away with the
10 thought of not just fixed cyber security
11 broadband, but also for mobile. And the benefit
12 will be faster response, quicker support to the
13 public, better response, better decisions and
14 actions and higher confidence. And I'd like to
15 say that in three and a half hours of this
16 scheduled call today, public safety probably
17 received on the order of over 100,000 9-1-1 calls.
18 Secure mobile broadband would have benefitted a
19 lot of those responses and I hope that one of the
20 things that happens here is that public safety
21 data in the field will see the kind of attention
22 commensurate paid to voice communications. And I

1 see this as a great first step and thank you very
2 much. The final comment I have is the
3 interoperability aspect. We hear it a lot on the
4 voice side. We do need it on the data side and so
5 I think a lot of people are paying attention up to
6 here and I appreciate it. So those are my
7 comments. Thank you.

8 MR. GOLDTHORP: Thank you, Allan. Let
9 me turn now to Dale.

10 MR. DREW: Thank you very much. So to
11 talk a little bit about -- about detection and
12 response from an internet service provider
13 perspective, and I want to echo a lot what was
14 said on panel number one as well. We, as an ISP,
15 do have -- our goal is to monitor as much data as
16 we possibly can to detect these threats, to
17 understand where they're trending, where their
18 moving, who's sourcing them, who's the victim of
19 them, why they are the victim and understand that
20 behavior so we can adjust the network and help
21 those victims and block the attackers as
22 appropriate. So, our goal is to be as proactive

1 as we possibly can, get access to as much data
2 within our network as we possibly can, you know.
3 And some of the challenges that we have, with
4 regards to that data, is there's data that's
5 pretty useful to us with regards to, you know,
6 collecting what we call netflow data, which is
7 sample traffic within the network and trying to
8 determine where that traffic is going and coming
9 from. The other one that -- that -- that we as
10 ISPs try to implement is deep packet inspections
11 to be able to look for, you know, specific threats
12 because these threats are becoming much more
13 sophisticated in nature, much more intense in
14 nature and getting more access to that data is
15 critical to understanding, you know, the nature of
16 those attacks. So, you know, I think that the
17 other thing that I want to stress here and I've
18 heard this echoed a number of times as well, is
19 the people component. You know, having the right
20 people in the right positions is pretty key and
21 training and testing of those resources is also
22 key to being able to -- not only be proactive --

1 have the skills and resources necessary to perform
2 the research, determine what the threats are --
3 but also have the skills and resources to be able
4 to respond to those incidents when they occur.
5 So, you know, we have multiple teams that are
6 focused on detecting what those threats are and
7 being proactive and collecting that data from the
8 good guys and the bad guys, determine what their
9 interests are, what -- how they're protecting
10 their infrastructure, understand that data, be
11 able to dissect that data and see where the trends
12 might be heading -- but also people who are able
13 to detect those events that are occurring --
14 either the ones that are pretty obvious or the
15 ones that, you know, that are not so obvious. So
16 -- you know -- so, in my mind, you know, training
17 -- training and testing is pretty key to this
18 element as well. And I'm blind and can't see my
19 slide. I will say that one of the challenges that
20 we have is that these attacks are becoming much
21 more social in nature, you know, so we -- you know
22 -- we do have the garden variety bot attacks and

1 the garden variety denial of service attacks and
2 those attacks are definitely still -- still being
3 invested in and still being sourced. But we're
4 also seeing the bad guys -- we're also seeing the
5 bad guys, you know, attack our employees and
6 attack our customer's employees. There's a fair
7 amount of information that we as a society put out
8 on the internet about ourselves -- the projects
9 that we're working on, the things that we're
10 investing our time in -- and those resources are
11 being exploited for the purposes of targeting
12 specific employees performing specific projects
13 within companies by creating zero day viruses,
14 social engineering attacks to try to gain access
15 to the infrastructure and those attacks are
16 extremely difficult to detect and extremely
17 difficult to stop. I said one of the things that
18 we have a benefit of is that at Level 3 we
19 recently combined the -- our security
20 organizations into a single organization so our
21 enterprise security, our product security and our
22 production security all into one, as well as

1 physical and logical. That centralization has
2 really provided a benefit for us in detecting
3 threats and attacks in a much more uniform way.
4 You know, we had, you know, as a company, we had
5 issue sharing information between departments, let
6 alone sharing information between agencies and
7 other organizations. So just combining that
8 information, coming up with a unified approach and
9 a unified standard has really provided us a
10 tremendous amount of assistance. With regards to
11 response, you know, there are plenty of -- I think
12 I want to go back one -- there are -- no I'm --
13 there are plenty of forums, both on the government
14 and on the industry side. What I'll say from an
15 IT perspective and I'm kind of going off my notes
16 here, but one of the challenges that we have is
17 that we have to implement whatever product that we
18 purchase and it's -- and I have not -- not seen
19 this dialog or discussion within the forum, but
20 getting more assistance from vendor capability is
21 going to be key to winning this war. So making
22 sure that we have the right capability in our

1 products -- whether they're consumer products,
2 whether they're backbone products -- is going to
3 be a major element for us leveraging those
4 resources and those capabilities to provide a more
5 unified approach to protecting our infrastructure.
6 We are often a victim of the infrastructure that
7 we deploy. We are often a victim of the speed
8 service that we want to offer to our customers and
9 as a result, you know, we tend to pick the
10 products that offer the best functionality and not
11 necessarily the best security. So making sure
12 that those -- those products, those services and
13 those vendors have a focus on the right level of
14 security I think is going to be pretty important.
15 And then with regards to information sharing, I
16 think that -- that, you know, we as an industry --
17 both with industry forums as well as the
18 government -- there are plenty of forums for us to
19 share information. With regard to the industry,
20 it's all about the circle of trust and making sure
21 that you can share information appropriately.
22 With the government, it tends to be everyone wants

1 to control their own data and so there's plenty of
2 forums to choose from within the government and so
3 trying to find a way to -- to unify that
4 information sharing I think is going to be key.
5 And that's all I have. Thank you very much.

6 MR. GOLDTHORP: Okay. Thank you, Dale.
7 We turn now to Andy. Would you like to say a few
8 words?

9 MR. OGIELSKI: Good morning. I am
10 honored to be here and I would like to thank FCC
11 and you, Jeff, for invitation. In my
12 presentation, I will focus on a sector of cyber
13 security issues dealing with the internet
14 infrastructure rather than with security and
15 vulnerabilities of the end systems that have been
16 so widely spoken about here. First of all, I
17 would like to point to the Commission and to the
18 audience that because of the way internet grew and
19 evolved from within academic research, it evolved
20 together with means to monitor it. So a third
21 party, such as our company, can actually monitor
22 the state of the global internet fairly

1 accurately, notice all outages, instabilities,
2 networks that are connected, networks that become
3 disconnected, and so on. We gain knowledge this
4 way that one of the several key capabilities that
5 are needed for service restoration is highly
6 accurate -- a who is who registry. Apparently
7 they are not very good as you all know. Finally,
8 I would like to point out and give you an example
9 that because of this highly automated nature in
10 which internet can be monitored, we can also think
11 about quantitative metrics that quantify the
12 quality and security of the infrastructure at
13 least -- not the end systems -- very difficult
14 that we have heard at previous panels. So, very
15 briefly about the nature of connectivity threats,
16 to which I will stick myself today. There are
17 physical problems -- anything from hurricanes and
18 earthquakes to intentional hostile destruction
19 acts -- in short, bombs and such. There are
20 routing vulnerabilities. They are not very well
21 known in our cyber security community, but the
22 truth is that there is only one protocol that

1 connects internet. It's called portal gateway
2 protocol. It's not secure. It can be easily
3 spoofed and it is being abused. And there --
4 there is no good path forward at the moment. And
5 lastly, but importantly in this forum -- business
6 conflicts from time to time, in peril,
7 connectivity among parties. Technically speaking
8 (inaudible) events. So, about monetary. What can
9 we see? This just a snippet from Katrina. We
10 have it for all major events on the internet since
11 2002. We can track exactly which networks have an
12 outage, where, how long, when the outages appears
13 and pinpoint it on the map. Regarding incidents
14 that illustrate potential of cyber attacks. Here
15 -- to repeat -- we are talking about the cyber
16 security of the infrastructure. So this will be
17 attacks on switches and routers -- not on end
18 systems. I just chose two incidents from very
19 many that we know. They happened because certain
20 vendor's routers just reset or die upon receiving
21 malformed messages from other routers. These were
22 not hostile attacks as far as we know, but look --

1 I mean a single a bad router somewhere in this
2 case either in Japan or in Czech Republic or in
3 Africa can raise the level of instability of the
4 global internet by a factor of 10 or more.
5 Imagine more. And there have been many much more
6 serious attacks on the routing infrastructure
7 typically based on injections of fake routes,
8 meaning -- one of the more famous ones, many of
9 you may know it -- was the attack on You Tube by
10 Pakistan. It was not intentional as far as we
11 know. Finally, these things can be measured
12 continuously. So just for illustration, we have
13 compared the agreement between routing registries
14 and actual routing as executed by every network in
15 the world in every country. U.S.A. (inaudible)
16 kind of in the middle, okay. China is not too far
17 away. Russia, I think, is well known for being
18 ruled with an iron hand, so they are pretty good.
19 I don't want to suggest anything. So, where are
20 we today and what we think are the trends? In
21 physical -- with physical problems, we believe
22 that based on observation and measurements --

1 because we are very data driven -- we believe that
2 (inaudible) is improving and initiatives such as
3 National Broadband Plan can only make it better,
4 because it's a redundancy of bandwidths in a
5 facilities that will protect us and enable faster
6 service restoration. With routing
7 vulnerabilities, it is not good. There is no
8 clear path toward secure routing that is available
9 at the moment. So the best we can do today is to
10 monitor all problems and respond quickly.
11 Regarding business conflicts, I figure in this
12 forum I would just like to point out that in
13 disruptions of service, in various countries, we
14 have seen the best recovery happened when there
15 was a large diversity of providers, because not
16 every provider fails the same way and recovers the
17 same way. And in light of the recent economic
18 troubles, I would say that maybe we should
19 consider how big is too big for network service
20 providers. There is a lot of examples of this
21 nature that we have worked out and given the
22 limitations of time, I can either talk to you

1 privately about it or you can go to this website
2 and find a lot of quantitative measured results.
3 So, thank you very much.

4 MR. GOLDTHORP: Thanks, Andy. Turn it
5 over to you, Phil, to --

6 MR. REITINGER: Thanks, Jeff. Welcome,
7 everybody. I'm a little cautious about doing this
8 because I look out in the audience and I think I
9 know fully a third of you. So, I'm always
10 cautious of the fact that, you know, sometimes
11 we're speaking to ourselves and we need to get out
12 broader. So I hope there are lot of people out
13 watching the Webinar that will take something from
14 this. So let me -- I'm going to speak I think
15 fairly briefly and at a relatively high level. I
16 want to start with one proposition which was
17 included in the President's Cyber Space Policy
18 Review that to me is undeniable, but I'm happy to
19 have a discussion about it if you want to. And
20 that is that the status quo is not sufficient. We
21 are in a very bad situation right now where
22 offense beats defense in cyber space and there's

1 not a whole lot we can get done about it. So
2 we've got to concentrate, among other things, on
3 moving from the state we're in right now to the
4 state of, you know, plus n -- now plus n. And I'd
5 like to talk a little bit about what I think that
6 means for cyber security and what I think that
7 means for communications. And I'll -- I'll sort
8 of reverse order. On cyber security, I'm going to
9 start with I think where we want to be and what we
10 need to do now and then I'll reverse it and say
11 where we are now on comms and where we want to be.
12 So, where we want to be in terms of cyber
13 security. We just need a fundamentally more
14 secure ecosystem. And I'd suggest I think that
15 includes a couple of things -- some ideas that
16 have already come up on this panel and I suspect
17 the panel before. One is we just need a much more
18 automated, interoperable mechanisms for doing
19 security. And that means both content and policy.
20 You know, we -- we need to do the sort of -- take
21 the groundbreaking work that is placed -- that has
22 taken place on things like the security content

1 automation protocol, for those of you who are
2 familiar with it, and put that kind of work on
3 steroids so that we have a highly interoperable
4 security ecosystem that lets us read and react and
5 mitigate in real time. The other thing I think we
6 need to go along with that is to build that more
7 effective ecosystem on a foundation of strongly
8 available and interoperable authentication because
9 with privacy built in from the very start, because
10 everything -- and (inaudible) postulate I'm also
11 happy to discuss -- everything on the internet is
12 action at a distance. Even if the software you're
13 running in your box, you can't see it and touch it
14 and feel it. So it's all action at a distance and
15 you can't make effective judgments about it unless
16 you know what it is, and -- or who someone is or
17 what a device is. So that doesn't mean everything
18 needs to be authenticated all the time by any
19 means, but it means it's got to be available and
20 interoperable when they want to do it if they want
21 to make effective security judgments. If we could
22 do those sorts of things, I think we will be in a

1 fundamentally more secure ecosystem. The question
2 is what we do about the situation we're in right
3 now. Obviously, because we've got an ecosystem
4 that was designed for availability and
5 reliability, but not security, we are inherently
6 in a reactive mode a lot of the time, which means
7 we've got to be really good at being reactive and
8 we've got to continue to get better at being
9 reactive while we try to get out of the game of
10 Whack-a-Mole. And some of the things I think that
11 means -- we're working several key initiatives on
12 that. A couple I'll highlight. We're -- we're
13 leading the effort -- it's a broad interagency,
14 intergovernment -- an effort with the private
15 sector to develop is called for in the President's
16 Cyber Space Policy Review, a National Cyber
17 Incident Response Plan that would truly enable the
18 public sector and the private sector to sort of
19 respond as one nation to incidents of national
20 significance. Another thing we're doing is while
21 I'm talking about comms and securities separately,
22 recognizing that comms and IT are

1 indistinguishable in -- you know, to me, now, but
2 I think to a lot of people, certainly in the mid
3 to long term. So we're collocating -- we have --
4 just within the organizations that report up to
5 me, we have a separate watch and warning center
6 for comms and IT. The NCC for comms and U.S. CERT
7 for IT. So we're going to be collocating in the
8 immediate future those centers with another center
9 that I'm a director of -- the National Cyber
10 Security Center, which is an interagency center --
11 all in the same place, bringing in more private
12 sector people over time. So we're building up an
13 integrated watch and warning capability that can
14 enhance the ability of the public and private
15 sectors to work together. With that let me lead
16 -- quickly transition to the comms because I spent
17 too much time on IT. I'd echo Allan's comments.
18 Public safety -- and I would say more generally
19 national security and emergency preparedness
20 communications have very, very unique needs that
21 we need to make sure we can meet as we go forward
22 on greater and greater broadband deployment.

1 We've actually got a whole spectrum of effective
2 programs right now. Allan talked to some of the
3 things they do in public safety. We've got things
4 that we do specifically on the NSEP front that I
5 would say, if I could generalize, are low
6 capability, high reliability mechanisms. There --
7 they don't provide the same sort of things that,
8 you know, people who carry, you know, smart phones
9 or PDAs have come to expect, but they give, you
10 know, that core communications. We're in a unique
11 point of opportunity right now as we go through
12 the period of convergence to make sure that we can
13 have our cake and eat it too for NSEP
14 communications. There's going to be a whole bunch
15 of things that packet-based communications are
16 going to enable and if we build security and
17 interoperability and reliability in from the
18 start, we're going to enable people from -- you
19 know, first responders, local fire and emergency
20 up through the highest level of, you know, secure
21 government communications to have broad
22 capability, broad interoperability and high

1 reliability at the same time. But we've got to do
2 that very notionally. It's not going to happen by
3 accident. And so I think there are things that we
4 could talk about on the way forward. I think the
5 best way to make that happen is a subject for
6 discussion. But I think we absolutely have to get
7 there. The other thing I point out is a key part
8 of that is going to be, you know, like we in the
9 internet rely on open standards for IP, for
10 packet-based communications, we're going to have
11 to rely on open standards for interoping that
12 space, too. Because we're all going to need to be
13 able to work together and the comms or the IT
14 infrastructure at internet speed and quite
15 effectively. So, I think I'll just -- I'll stop
16 at that point and be happy to participate in
17 questions when the panel is done.

18 MR. GOLDTHORP: Okay. Thank you, Phil.
19 And thank you to our other panelists for our
20 opening remarks. We have a group of FCC panelists
21 here to ask questions. We also have an audience
22 here in the room and we have an audience on the --

1 on the Webinar, and so we'll be taking questions
2 from all three sources. But, let me start with
3 the FCC panel. Before I do, before I do -- I
4 don't -- Allan, I don't want to -- you're not on
5 the screen right now, but if there's a question
6 that comes up that you want to answer to, I'll try
7 to remember that you're there and pop you in.
8 There you are. But just speak up, okay? And --
9 so --

10 MR. OGIELSKI: Okay.

11 MR. GOLDTHORP: Thank you. Let me ask
12 if there's any questions from the FCC panelists
13 first. John?

14 SPEAKER: So, Andy Ogielski -- I'm sorry
15 if I've mangled that -- raised, you know, talked
16 about routing vulnerabilities and raised the issue
17 of BGP. Actually, I could have picked examples of
18 authentication or other things that you brought up
19 for this question, but I'll use BGP. This is
20 something we've been hearing the ITF and the
21 research community talk about for more than a
22 decade certainly -- some of the vulnerability,

1 some of the things that could be done in response
2 to those vulnerabilities. I'm going to ask if are
3 service providers at this point doing all that
4 they can -- all that we know how to do to address
5 this issue and if not, is there something that
6 government could do -- perhaps in a national
7 broadband plan -- to assist or enable or motivate
8 them to take other steps?

9 MR. OGIELSKI: Maybe I'll just start
10 answering and then defer to the others to complete
11 it. There are -- first of all, in order to make
12 progress, we -- the operators and users of the
13 internet -- have to know what is the ground truth
14 -- who owns what. It is not available. So if,
15 for instance, your network address out of the blue
16 becomes advertised or originated say in Malaysia,
17 very few people will notice. That's why You Tube
18 was hijacked. It was very, very famous event.
19 Two -- yes, there is at least two advanced
20 research projects that, I think, have lasted
21 longer than 10 years to create secure routing
22 protocols. They are not practical and there is no

1 manageable path forward. We will not have a flag
2 day on the internet today with everybody switching
3 over to a new protocol overnight. It's nice to
4 say that it would be good for research to pick it
5 up, but research has been working on it and simply
6 there are no results. I don't think anybody would
7 like government intervention here because it's a
8 global problem. We cannot just solve it in the
9 U.S. and let it be as it is elsewhere. So, maybe
10 other panelists would contribute as well.

11 SPEAKER: More research, I guess, but
12 the BGP problem is well known and it's lethal and
13 -- yeah, he's right.

14 SPEAKER: Isn't it largely well known --

15 SPEAKER: Talk into the mic, sir.

16 SPEAKER: -- to some extent, it's a
17 first adoptive problem. I mean it doesn't do
18 anybody like Level 3 to go out and put security
19 BGP in their network if nobody else does it. So
20 that seems like the classic environment in where
21 -- and I'm not saying I disagree with your
22 assessment, but if there's any environment where

1 government has a role to step in, it's to kind of
2 overcome those first adoptive problems. Now it
3 may not be that that's the right solution and I'll
4 -- it may be that there are simpler solutions for
5 securing, you know, the interprovider links and
6 whatever that would make a big difference -- that
7 may or may not be being done, but I guess I'm at a
8 loss when you say you don't want to see government
9 step in. Well, how -- but also that there's no
10 solution so.

11 MR. OGIELSKI: Just to comment.
12 Securing BGP is unlike securing DNS. DNS could
13 have been secured and it is being secured as we
14 speak. Because the upgrade is compatible with the
15 existing systems. It is not the case with
16 routing. Second, even if here in our country, we
17 would mandate say that all our providers and great
18 companies like Google, must use secure BGP
19 effective say January 1, please keep in mind that
20 all large networks span continents or the globe,
21 so there is no local solution to this problem.

22 SPEAKER: I would also -- I would agree

1 with the panel that -- that -- that as service
2 providers, we are patching the issue as opposed to
3 solving the issue. But it's not just a protocol
4 issue, it's also that there's a degree of inherent
5 trust with ISPs, how they route traffic, how they
6 advertise traffic. And so in order to secure the
7 protocol, you have to determine whether or not you
8 want to remove that trust and to what degree you
9 want to take that trust out. So, just saying that
10 we want to secure the protocol only solves for
11 half the problem. We need to, determine as ISP
12 communities, what level of trust we're going to
13 have when we pair with another provider.

14 SPEAKER: Even within the existing
15 protocol, there are things can do, right? One can
16 filter or one cannot filter --

17 SPEAKER: Absolutely. So today we have
18 -- we have check sums in place to ensure that no
19 one can attack the protocol itself. We have route
20 filters to ensure that other ISPs can't take over
21 large blocks of addresses that they don't own. I
22 mean, so there are patchwork processes to help

1 incrementally improve this issue, but the reason
2 why this has been such a fundamental problem
3 because it is -- you -- the act of pairing with
4 another provider means that you are -- you are
5 assuming a degree of trust with that other
6 provider and when that provider decides to take
7 advantage of it. So when another country who owns
8 their address space says anyone within my network
9 when they go to Google -- Google or You Tube or
10 whatever -- are now going to go over here rather
11 than the real Google or the real You Tube. They
12 have that degree of control and removing that
13 control from themselves is going -- is the
14 problem.

15 SPEAKER: I was going to just generalize
16 briefly. Not to answer the BGP problem in
17 deference to my colleagues who are far more expert
18 than that, but, you know, the issue of the problem
19 of first adopters came up. I -- I think we do see
20 regularly on the internet -- and I'm not calling
21 for regulation or nonregulation in any particular
22 place, but less of a first adopter problem and

1 more of what I would call a collective action
2 problem. And identity management or
3 authentication is one of those areas that we need
4 to pay attention to, because if there are places
5 where multiple disconnected parties with
6 misaligned incentives need to move simultaneously
7 to accomplish an end result -- that makes it much
8 harder in the ecosystem. That sort of thing does
9 not arise organically. And so government in those
10 cases, I think, does need to look at how to help
11 bring about the result -- how to catalyze
12 ecosystem movement that could move us to a more
13 secure end state.

14 MR. GOLDTHORP: Let me move to a
15 question from the -- from --

16 MR. OGIELSKI: If I could just briefly
17 comment. What we also see is that the global
18 operator community is incredibly quick in reacting
19 problems with BGP. I mean, I show this as two
20 peaks of things that look like attacks, but
21 weren't. You couldn't see the time scale, but by
22 informal communication channels, operators around

1 the world essentially shut down the offending
2 provider within half an hour to an hour. So the
3 level of cooperation among network service
4 providers is exemplary.

5 MR. GOLDTHORP: Okay. Thank you. We
6 have question from the web now from Jeremy. And
7 let me -- let me preface this by -- the context
8 here is as we move to more of an IP based
9 infrastructure, the -- and we're thinking now
10 about cyber security. Some of the bigger concerns
11 have to do with the fact that infrastructure will
12 be used to carry critical communication services
13 like 9-1-1. So think about next generation 9-1-1
14 and as I ask this question -- in light of the
15 decentralized nature of the public safety
16 industry, where state and local governments
17 mandate and control their networks and security is
18 a widely varied -- is implemented in a widely
19 varied manner on 9-1-1 networks, would we look --
20 should we look to the federal government to bring
21 some sense, some commonality or common set of
22 standards for next generation? And I added -- I

1 think that's what is meant here -- for next
2 generation 9-1-1 networks. Or should we continue
3 to rely on state and local agencies to understand
4 and enforce cyber security on their own?

5 MR. SADOWSKI: I'm game. This is Al
6 Sadowski.

7 MR. GOLDTHORP: So this is now thinking
8 about a very specific and important service
9 running on these infrastructure.

10 MR. SADOWSKI: Was that deferred to me?

11 MR. GOLDTHORP: Yes. Thank you, Allan.

12 MR. SADOWSKI: The -- I'm game on this
13 one. Yeah, I think standards are critically
14 important so I do like that statement. And I
15 think that if -- as long as we defer to the tens
16 of thousands of organizations that are involved in
17 9-1-1 -- the peace apps, the public safety access
18 points. As long as they each get to go it their
19 own way, it is unlikely that we're going to
20 achieve any consistency. So I think there would
21 be some benefit. A good question and I think it
22 would be beneficial for standards on the next

1 generation to do that and to include certain
2 entities that are not traditionally on the peace
3 at world today -- that are not the 9-1-1 answering
4 point, but, in fact, the 9-1-1 answering point
5 relays the call over to some of the entities. So
6 there's a lot of the first responders who don't
7 get that location information, that don't get the
8 identification information and that would be
9 helpful. So yeah -- I think that's a standard to
10 make it consistent and to extend it to additional
11 actors in the first responder world would be a
12 great benefit.

13 SPEAKER: So I'll just make a couple
14 points in addition to Allan's. I mean the
15 question seemed to propose or presuppose -- and
16 maybe it didn't, but I read it as perhaps
17 presupposing that this is an area that would
18 involve federal top down solutions. And I'm -- I
19 would I think disagree with that if that's --

20 MR. GOLDTHORP: We're just questioning
21 if that would help?

22 SPEAKER: I think one, we need a joint

1 vision. We need a common vision among emergency
2 preparedness communicators and, you know, both
3 within the federal and the states on where we want
4 to go. I agree with both Allan and the point of
5 the question that we need common standards to
6 drive interoperability and capability --
7 absolutely. I would say that that is less likely
8 to arise from top down requirements and more from
9 providing assistance and bottom up -- you know,
10 voluntary creation of standards that actually meet
11 the needs of the first responder community. It's
12 a very distributed community that has highly
13 specific requirements and I think it is incumbent
14 upon us to work broadly -- you know, both at the
15 federal and state level -- with the different
16 participants to ensure that we create a set of
17 standards and solutions that actually meet their
18 needs.

19 DR. DONNER: So let me -- let me sort of
20 challenge some of the thinking with a question.
21 We recently implemented a -- what's called a one
22 box -- for poison control. So, if you in the

1 U.S., if you search for poison control, you'll get
2 the one box that says here's the poison control
3 number. We have, for a substantial amount of
4 time, been interested in implementing a -- you
5 know, if you search for emergency room, provide
6 some sort of access to information about that.
7 But what we've discovered is that a comprehensive
8 list of emergency rooms is not, in fact, in
9 existence. So the -- one of the reasons why this
10 broad distributed network of response
11 organizations exists is party to create the local
12 directory because someone on the ground locally
13 can do that and to -- and to be part of the
14 response organization to roll trucks and cars and
15 things like that. But it is not, in fact,
16 necessarily the case that the most efficient thing
17 in the world to do is to have telephone banks
18 scattered hither and thither across the entire
19 country to handle all those calls. So you might
20 consider thinking about a rich, very
21 comprehensive, very accurate supply of data that
22 many different operators could use to respond to

1 first calls.

2 MR. GOLDTHORP: Okay. Thank you, Marc.
3 Let me -- Jean Ann, do you have a question? Go
4 ahead.

5 MS. COLLINS: Okay. There's been a lot
6 of general discussion today about collaboration
7 between companies and public-private collaboration
8 with respect to cyber security and the need for
9 incentive or motivation to better achieve this
10 collaboration. And, in fact, Mr. Reitingger
11 recently spoke about his work towards an
12 integrated --

13 SPEAKER: Microphone closer.

14 MS. COLLINS: Closer?

15 SPEAKER: Yes.

16 MS. COLLINS: -- an integrated watch and
17 warning capability. My question is two part and I
18 do have a question. First is could you describe,
19 to the extent possible, how you currently
20 coordinate with industry and government with
21 respect to detecting and responding to cyber
22 attacks? What forms you find most beneficial?

1 And the second part is could you discuss any
2 recommendations you have for improving this
3 process in an attempt to achieve, you know,
4 real-time information sharing and coordination
5 between the numerous forums that people have been
6 speaking of?

7 MR. GOLDTHORP: Who was your question
8 directed to again?

9 MS. COLLINS: Anyone who wants to
10 answer.

11 MR. GOLDTHORP: Oh, anyone. Okay. I
12 thought you said it was to Marc. Okay. Anyone?
13 Why don't you start, Dale?

14 MR. DREW: I'll address at least half of
15 your question. On the area of improvement, I
16 think one of the things that -- that we're really
17 trying to focus a lot of time on -- with our
18 vendors, with our partners -- is trying to unify
19 the information that we want to share with each
20 other. So, the products that we use, the vendors
21 that we use -- there is -- the data that they
22 present is not normalized in any way. So we have

1 to invest in infrastructure and resources and
2 expertise to try to -- try to normalize what those
3 attacks are and collaborate that data across those
4 very disparate data sets and that tends to cost
5 more resources than -- than -- you know -- than
6 the threat itself. So trying to find a unified
7 messaging format for -- for our vendors as well as
8 a unified information sharing format -- to share
9 information across each other because we all have
10 different interests. We all have different areas
11 of focus and if we can start collecting that data
12 together and start sharing that data together, we
13 can have a more unified view of the total
14 universe. So, you know, I, as an ISP, don't --
15 don't tend to have broadband consumers on my
16 network, so I focus on -- my view is more on the
17 -- on the server side. Whereas other ISPs are
18 going to have the broadband users and they're
19 going to be focused on the Is. Sharing that data
20 together to try to unify attack signatures is
21 going to be a big step for us being able to
22 respond to those attacks a lot quicker.

1 MR. GOLDTHORP: Dale, let me follow up
2 on that for a second because this is interesting.
3 You know, years ago, in the telecommunication
4 sector, there was a lot of work that was done
5 between or amongst carriers to coordinate and
6 develop standards for things like electronic
7 bonding and so that there could be intercarrier
8 communication electronically and, you know, the
9 protocols and the data formats -- that was all
10 standardized so that carriers could -- in that
11 world, in that generation they could interconnect
12 and it was -- things were seamless so to speak,
13 right? And it seems like we have a problem now
14 that's similar in a sense that we're talking about
15 data that's available to corporate entities that
16 have some incentive at least to maintain the
17 privacy of that information. I mean at least
18 there's that -- that -- that's in there --
19 somewhere. And so I guess what I'm wondering --
20 yet, still, even though you have that -- there's
21 that issue to deal with, there's an incentive to
22 try and work together to be able to share

1 information. That's what I hear you saying. So
2 why can't there be some kind of a forum by --
3 through which these sorts of things could be
4 standardized? Maybe there is and I just don't
5 know about it.

6 MR. DREW: There is activity. There is
7 work to try to -- to unify that data together.
8 But there isn't a large incentive to do it.

9 MR. GOLDTHORP: What would it take to
10 create the incentive?

11 MR. DREW: I believe that over time the
12 -- I believe as the techs are evolving, I think
13 we're all discovering and I think one of the
14 reasons why these panels exist is because we're
15 all beginning to discover that -- that these
16 attacks are -- are more focused on -- on how the
17 infrastructure interoperates together as opposed
18 to attacking specific elements of the
19 infrastructure. And because of that, you have to
20 have a unified data approach. You have to be able
21 to look at the larger picture and how they all
22 interrelate. I mean the thing that struck me --

1 as the first panel was talking about how to
2 protect grandma's computer was that -- you know,
3 just in that example alone is that, if -- if there
4 was an incentive on the software vendors to ensure
5 that -- that security products were deployed,
6 could not be disabled necessarily by the consumer,
7 were offered, you know, either for free or some
8 cost that was -- that would incent the consumer to
9 use it, that the ISP had a capability of
10 validating that that was in place, that union of
11 the software vendor working with the ISP working
12 with the end user together would help resolve some
13 of those threats. So, you know, so I do believe
14 that there is -- we are talking with threat
15 vendors to make sure that the threats that they
16 publicize are in a unified format, that log
17 vendors have their information in a unified
18 format. So there is that direction. There is
19 that movement.

20 MR. GOLDTHORP: Okay. Good. Phil?

21 MR. REITINGER: I'll take a crack I
22 think at trying to answer both those questions.

1 So and the answer may be unsatisfying -- at least
2 to the first. I think it varies. The -- we, for
3 example, work with different entities throughout
4 the private sector -- from particular alliances to
5 the ISAFs to particular vendors as the case may
6 be. In point of fact, you know, every incident is
7 different to some degree or another and who needs
8 to be involved in responding to the incident can
9 vary significantly. I can say that, you know,
10 among the organizations we work with and those
11 that work within themselves, I think the ones that
12 are the most effective are the ones that have
13 built trust among their members. I used to like
14 to say the dirty little secret of information
15 sharing is it's all person-to-person and trust
16 based. And that is I still -- I think still
17 substantially true. A lot of information sharing
18 is based on -- and will be for the foreseeable
19 future -- on those trust-based relationships. But
20 because it varies from case to case, the key point
21 is that we need to have an agile system that will
22 allow you to collect the people who need to be

1 involved first in respond -- in mitigating an
2 incident and discovering a solution. And then
3 second, in responding to the incident. And that
4 could be a broader group of people in the second
5 case. In terms of the way forward, I think we
6 probably need to focus on three things. First is
7 continuing to build the relationships, the
8 organizations and the mechanisms that will allow
9 us to collaborate rapidly. So that's the -- sort
10 of the infrastructure of collaboration. The
11 second thing is we need to continue to focus on
12 removing barriers and increasing ROI or return on
13 investment for information sharing in particular
14 cases. You know a lot of the time we've focused
15 unduly on the removing barriers and not thought
16 about what's the ROI. Because a company -- you
17 know, a company is going to do things, because
18 companies -- companies have the national interest
19 at heart, too. But there's only so far they can
20 go without ROI. So we've got to build ROI so
21 there's value on built being in partnership
22 amongst companies or with government. The last

1 thing is we have to focus very specifically on
2 outcomes and cases rather than on the general
3 topic of information sharing. I've been involved
4 in these discussions since I think 1995 and it's
5 wonderful to come to meetings and talk about
6 information sharing and all agree that information
7 sharing is critical and then come back six months
8 later and have the same meeting where we all agree
9 on the value of information sharing. That doesn't
10 get us anywhere. We need to think about -- you
11 know -- what do we want to do? In a particular
12 case, what data do we want to be able to share?
13 What are the outcomes we want to drive? I
14 definitely -- I'd start with the outcomes. What
15 are the objectives? What data do we need to be
16 able to share to get to that objective and how do
17 we remove the barriers and the ROI and build the
18 ROI so that the mechanisms that we built, that
19 infrastructure of collaboration that we've got
20 will allow us to be effective. So that's my
21 action plan.

22 MR. GOLDTHORP: Okay. Thank you, Phil.

1 I'm going to turn now to the audience and ask if
2 anybody in the audience has a question. Please
3 raise your hand and Elaina will come around with
4 the mic and --

5 SPEAKER: Good morning. Rodney Petersen
6 with Educause. Since it was conceded that
7 securing DNS might be a plausible solution, I
8 wonder what the national broadband plan might say
9 about domain name system security or DNSSEC? As
10 we know, .gov through its own government mandates
11 are moving toward securing that domain. The
12 public interest registry has announced the same
13 for.org and Educause, with the Department of
14 Commerce, just two weeks ago announced the plans
15 to implement it for.edu. So I wonder what the
16 national broadband plan might say about DNSSEC
17 and, more specifically, what the role for carriers
18 might be?

19 MR. GOLDTHORP: Why don't you start,
20 Dale?

21 MR. DREW: Well, from a carrier
22 perspective, our interest is to ensure that we

1 provide the infrastructure that our customers
2 want. So as an example, it was because of -- of
3 universities and the government interests in IPv6
4 that we as carriers are implementing IPv6. And
5 it's the same for DNSSEC. There are a significant
6 number of challenges to overcome with DNSSEC from
7 a carrier perspective, but, you know -- but the
8 issue is from a -- from a carrier perspective,
9 that -- that as those customers -- the
10 universities, the governments and so on -- want
11 those services, we as carriers are going to be
12 implementing them. I can't speak for the national
13 broadband plan though.

14 SPEAKER: I can't speak for the plan
15 either. I have a follow up question. And I guess
16 the question would be to what extent does DNSSEC
17 solve sort of DNS problems you see? That is
18 there's clearly a class of problems, but there
19 must be -- you know -- what is the sort of balance
20 between the sort of the brute force attacks on the
21 DNS system, which we certainly see at the root
22 level from time to time, versus, you know, the

1 more sophisticated, you know, hijacking of routes
2 and whatever? Do you have some sense of that or
3 -- you know -- how much does DNS solve -- DNSSEC
4 solve the kinds of problems that are confronting
5 the DNS system?

6 MR. GOLDTHORP: Andy, why don't you take
7 a crack at that?

8 MR. OGIELSKI: That's I think risky,
9 okay. I would say that I'm really looking in two
10 -- at two emerging areas. One is appearance of
11 commercial DNS service providers -- either paid or
12 offering the services for free. And there are
13 several companies of this type. And that's a very
14 interesting development because in this way an end
15 user even with a modicum of skills can get their
16 DNS replies from somebody they trust, rather than
17 from some random operator who services this
18 particular hotel or that particular coffee shop.
19 So that's one. Two -- I think it's worth adding
20 so this is not an answer. It's a broadening of
21 the question. By chance, DNS is such a convenient
22 protocol, that it is used in a very large number

1 of situations where nobody imagined DNS is going
2 to be used. And among others, I think Dan
3 Kaminisky recently made a lot of splash showing
4 how many vulnerabilities there are beginning with
5 simple thing when you want to change password in
6 your service. How do you think your computer
7 finds the site where it gets a new password from?
8 Well, through DNS. So securing DNS has much
9 broader impact I think and unfortunately I cannot
10 answer fully whether DNSSEC will solve all these
11 problems.

12 MR. GOLDTHORP: I want to make sure that
13 we're answering the original question. Is this
14 getting to where you wanted to go? Okay. You
15 know, we've got about four minutes left and unless
16 -- unless somebody is dying to ask a question,
17 there's something I've been dying to ask since I
18 walked in the door, okay? And it's this. Four
19 minutes is enough time for five people to make an
20 elevator talk and so what I'm wanting to know is
21 what would your elevator talk be? Maybe it's a
22 three floor elevator, right? Not a big one. If

1 we were going to put anything -- if there's
2 anything in this national broadband plan that
3 would address the issue of cyber security, what do
4 you think it should be? How should the plan
5 address cyber security? What are the two or three
6 or one or two things that should be in there?
7 What do you think, Marc?

8 DR. DONNER: I -- that's a really good
9 question and I don't have -- let me just think
10 about that for (inaudible) --

11 MR. GOLDTHORP: This is what elevator
12 talks are like.

13 DR. DONNER: I can't do it.

14 MR. GOLDTHORP: You never know what is
15 going to get asked.

16 DR. DONNER: I think there's several --
17 several of my colleagues have made excellent
18 proposals. I think BGP is key. I think dramatic
19 improvements in the use of authentication are the
20 biggies that are going to make the most important
21 difference.

22 MR. GOLDTHORP: Okay. Thank you.

1 Allan, what do you think?

2 MR. SADOWSKI: Basically two things from
3 a public safety perspective. The redundancy that
4 the networks are going to have to have even if
5 that redundancy is just for public safety and
6 well, the -- I think possibly -- I mean, public
7 safety may have to do a carve out much like DOD
8 does with SIPRNet -- maybe for mission critical
9 public safety may have to be a part of it. I'll
10 keep it short. Those two things.

11 MR. GOLDTHORP: Okay. Thank you. How
12 about you, Dale?

13 MR. DREW: I would focus on two things.
14 I would focus on proactive information sharing. I
15 think that we as an industry are getting really
16 good at reactive information sharing. I don't
17 think we should stop that. But getting -- getting
18 better at sharing information before the actual
19 incident occurs is key. I think the other one is
20 -- is putting a bit more responsibility on the
21 vendors who provide the products to ensure that a
22 degree of security is built in to the

1 infrastructure before it's available. All the
2 standards that are available, all the focus that
3 we've had is how do we protect the thing that we
4 have as opposed to how do we ensure that it's
5 protected when we receive it.

6 MR. GOLDTHORP: Okay. Thank you. Andy?

7 MR. OGIELSKI: I would say that only one
8 requirement on expanded national broadband service
9 would go a long way and that is I want to have
10 guarantees that I'll always have this bandwidths.
11 If that's provided, then a lot of other problems
12 have to be solved.

13 MR. GOLDTHORP: Okay. Phil?

14 MR. REITINGER: So on the -- I'm a
15 little less comfortable in sort of identifying in
16 cyber security what ought to be in the plan or not
17 in the plan. I think I'd take what Allan said and
18 broaden it a little bit. Without saying a
19 particular solution should or should not be in the
20 plan, it seems to me that we -- as I said in my
21 opening comments -- need to ensure that as we move
22 forward with broadband deployment and broader use

1 by both national security and emergency
2 preparedness communicators, that we don't move
3 from a world of low capability, high reliability
4 to a world of high capability, low reliability.
5 But instead move to a world of high capability,
6 high reliability.

7 MR. GOLDTHORP: Okay. Thank you all.
8 We're at a point where we've got to bring our
9 panel to a close. I wish we had some more time
10 because there are some questions we're just not
11 going to get to and so I apologize to both Cynthia
12 and Carolyn for not being able to take your
13 questions today. But as we did before, these will
14 be recorded and we thank you for your questions.
15 Thank you to the audience as well for being here
16 and for your questions. And a special thanks to
17 our panel, our panelists and for your contribution
18 today. So --

19 MS. MANNER: -- and our moderators. I
20 think this was a great day of conversation that
21 we've had. We appreciate our participation here
22 in D.C. and also those who participated in the

1 Webinar. I would like to call people's attention
2 -- two days ago we released a public notice where
3 we've asked for additional public input on cyber
4 security issues and we would very much look
5 forward to hearing from everyone on those issues.
6 So this is going to go into the public record.
7 We're also going to follow up with our panelists
8 with some additional questions that were still
9 remaining. So thank you very much and have a good
10 afternoon.

11 (Whereupon, the PROCEEDINGS were
12 adjourned.)

13 * * * * *

14

15

16

17

18

19

20

21

22

1 CERTIFICATE OF NOTARY PUBLIC

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

14 /s/Carleton J. Anderson, III

15

16

17 Notary Public in and for the

18 Commonwealth of Virginia

19 Commission No. 351998

20 Expires: November 30, 2012

21

22

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

