

TRANSCRIPT OF PROCEEDINGS

In Re:)
)
COLLOQUIUM ON THE PUBLIC)
SAFETY AND THE HOMELAND)
SECURITY PORTION OF THE)
NATIONAL BROADBAND PLAN)

Pages: 1 through 50
Place: Washington, D.C.
Date: March 31, 2010

HERITAGE REPORTING CORPORATION

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

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

In Re:)
)
COLLOQUIUM ON THE PUBLIC)
SAFETY AND THE HOMELAND)
SECURITY PORTION OF THE)
NATIONAL BROADBAND PLAN)

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

Wednesday,
March 31, 2010

The parties met, pursuant to the notice of the
Commission, at 9:31 a.m.

APPEARANCES:

On behalf of Public Safety and Homeland Security
Bureau:

JENNIFER MANNER, Moderator
Deputy Bureau Chief

JAMES ARDEN BARNETT, Jr.
Chief

JEFF COHEN, Esquire
Senior Legal Counsel

LISA FOWLKES
Deputy Bureau Chief

DAVID FURTH
Deputy Bureau Chief

JEFF GOLDTHORP
Chief, Communications Systems Analysis

APPEARANCES: (Cont'd)

JOHN HEALY
Communications Systems Specialist
Communications Systems Analysis Division

BRIAN HURLEY, Esquire
Attorney Advisor
Policy Division

KENNETH MORAN
Senior Deputy Bureau Chief

1 proud to have him working with us. And I might add,
2 one of the reasons -- not only because he's a Marine
3 and I'm Navy, and we've worked -- believe it or not,
4 Navy and Marine Corps works together. The other thing
5 that I am very proud about is this is a guy with
6 public safety experience. And so we are -- in his
7 civilian life. So we really appreciate it. And
8 welcome aboard, Bill.

9 (Applause.)

10 MR. BARNETT: One other quick acknowledgment
11 for the good of the order, and particularly that you
12 would have some interest in. I'm going to ask Gordon
13 Fullerton to step up here with me for just a second.
14 And as he comes up, as you know, Gordon Fullerton is a
15 long-time public servant. Please come up and stand
16 here by me, Gordon. A long-time government servant.
17 And I found out recently -- please stand with me so
18 they can get you on camera here. I found out recently
19 that he is retiring, I guess you could say, from FEMA,
20 although I think this is, what, your --

21 MR. FULLERTON: Second time.

22 MR. BARNETT: Second or third retirement.

23 MR. FULLERTON: Yeah.

24 MR. BARNETT: And going to Booz Allen, where
25 he will continue important work in emergency

1 communications. Gordon retired after a long
2 government service. He was called back to help stand
3 up a new agency in the government. What was the name
4 of -- oh, the Department of Homeland Security, right.
5 So he actually helped stand that up, and then was
6 called back again regarding Katrina.

7 He has been instrumental in I guess bringing
8 a great deal of energy and efficiency to emergency
9 support function number two, the communications
10 restoration. And more than that, he has been a
11 tremendous friend to the Federal Communications in our
12 work. He was instrumental in the establishment of the
13 Project Roll Call that had its genesis during
14 Hurricane Katrina and has played significant roles in
15 subsequent hurricanes and disasters. It was deployed
16 to Haiti for the earthquake. And so there are so many
17 things like that that you have done for us. We will
18 miss you tremendously, and congratulate you on the
19 tremendous government service. Best wishes at Booz
20 Allen Hamilton.

21 MR. FULLERTON: Oh, thank you, sir.

22 MR. BARNETT: Thank you.

23 (Applause.)

24 MR. FULLERTON: I just want to take a second
25 to thank the FCC for all the great work they have done

1 in the last few years getting things going in
2 emergency communications. It has been a wonderful
3 time back. So thank you, sir.

4 MR. BARNETT: Thank you. Appreciate it.
5 With that, let me move into just a couple of comments
6 as we kick off right here. The people that you see up
7 here, a lot of people in the room, including
8 yourselves, have had input into the public safety
9 portion of the broadband plan. Of course, we have
10 heard a lot about the public safety broadband network
11 most recently. Probably the biggest ask that is in
12 the plan, particularly money -- and there are a lot of
13 matters that draw interest. There is a lot more in
14 the plan.

15 You'll get to hear the full spectrum of that
16 today. And I'm excited about it. So in addition to
17 public safety broadband network, you're going to hear
18 about plans for 911, for emergency alerting, for cyber
19 security, and other things that we are doing, all of
20 which fit together, all of which are extremely
21 important.

22 Now I might add that those of you who have
23 been around Washington, D.C. and probably other places
24 like that for a long time understand what can happen
25 to a plan. It can stay on the shelf. That's not

1 going to happen on this particular plan. And the
2 reason for that is that there is a good portion that
3 we have thought about that we need to work with other
4 government partners with or other pieces of the
5 government. There is a good portion that the FCC has
6 to do. We're moving out on that sharply, and that's
7 one of the things you'll start hearing about, is even
8 within a matter of days, weeks, and months, these
9 things are being timed that will start happening.
10 You'll get to see them and hold us accountable for
11 that.

12 And so without any further ado then, let me
13 turn it over to Jennifer Manner, who is going to
14 moderate our panel today. And thank you again for
15 being here.

16 (Applause.)

17 MS. MANNER: So let me echo Jamie's thanks
18 for you attending today. Just to give you a brief
19 overview of the format, each of our panelists is going
20 to talk about a different section of the Public Safety
21 and Homeland Security Bureau -- or I'm sorry, chapter,
22 of the broadband plan. And then we're going to open
23 the floor up for questions.

24 So with that, I'd like to start with David
25 Furth, who is going to talk about the nationwide

1 interoperable public safety broadband network. David.

2 MR. FURTH: Thank you. And do we have the
3 slides to start? Great, okay. Thank you and good
4 morning.

5 The first set of public safety
6 recommendations in the national broadband plan relates
7 to the development of a nationwide interoperable
8 public safety broadband network in the 700 megahertz
9 band. It's important to note at the outset that the
10 creation of this network has been an important
11 commission priority since before the plan was
12 initiated. As you may be aware, the 700 megahertz
13 spectrum has been made available for mobile broadband
14 use as a result of the digital television transition.

15 Congress has set aside a portion of this
16 band for use by public safety while allocating other
17 portions of the band for commercial use. In 2007, the
18 Commission determined that 210 megahertz of the public
19 safety spectrum would be dedicated and licensed for
20 broadband use. A second 10 megahertz block known as
21 the D block was slated by Congress for commercial sale
22 through an auction.

23 The Commission originally proposed a public-
24 private partnership in which the auction winner of the
25 D block and the national public safety licensee of the

1 adjacent public safety broadband spectrum would build
2 a shared network. However, the D block auction was
3 not successful, so that partnership did not
4 materialize.

5 In the national broadband plan, we are
6 proposing a new three-pronged approach for making the
7 national broadband public safety interoperable network
8 a reality. Go to the next slide. Let's see if this
9 works. Ah, yes, okay. This may be a little hard to
10 read, but we'll obviously make it available on the web
11 and elsewhere. The objective of the proposal is to
12 create a network that meets public safety's needs for
13 technological innovation, nationwide coverage,
14 interoperability, reliability, and affordability.

15 The first slide illustrates the three prongs
16 of the proposal. First, an administrative and
17 technical framework that will enable public safety
18 users to effectively use the public safety broadband
19 spectrum, but also to take advantage of commercial
20 broadband networks and technology that are developing
21 at the same time. Second, an emergency response
22 interoperability center, which we refer to as ERIC,
23 established to ensure nationwide interoperability and
24 operability of the network. And third, a program for
25 public funding to provide needed funding for

1 deployment and ongoing costs for the network. And
2 I'll briefly go over each of these three components.
3 I would also mention that the first two are primarily
4 for follow-up action by the FCC. The third would
5 require action by Congress.

6 Going to the first prong of the plan, this
7 is based on the concept of what we call flexible
8 incentive based partnership. What this means is that
9 public safety entities can choose who to partner with
10 in building the corp public safety network. They can
11 partner with a public commercial provider, including
12 but not limited to the D block licensee, or can seek
13 to build on their own.

14 We also recognize that at times public
15 safety broadband users may need the ability to roam
16 onto other networks or to obtain access to additional
17 capacity. Therefore, the plan recommends giving
18 public safety the right to roam and obtain priority
19 access on commercial networks in 700 megahertz and
20 potentially other bands at reasonable cost.

21 This element of the plan not only adds
22 capacity, it also adds resiliency and redundancy by
23 enabling public safety to use multiple networks rather
24 than relying on a single network. The plan assumes
25 that the D block will be auctioned for commercial use,

1 but with two conditions that create incentives for
2 partnership and lower public safety costs. The first
3 requirement is that the D block licensee or licensees
4 will be required to use the same air interface as the
5 public safety network. The second requirement is that
6 the D block licensee or licensees must develop user
7 devices capable of operating across both D block and
8 the public safety spectrum. The plan also recommends
9 that commercial providers and other bands be required
10 to support development of similar multiband equipment
11 that operates in the public safety spectrum as well as
12 their own bands.

13 The second element of the proposal is ERIC,
14 which we propose to create within the Commission.
15 ERIC will be a technical body staffed primarily by
16 engineers. It will work with both public safety and
17 industry to establish nationwide standards for
18 interoperability on the broadband network. ERIC will
19 work closely with DHS's Office of Emergency
20 Communications and with the National Institute of
21 Standards and Technology in carrying out its mission.

22 In addition, a public safety advisory
23 committee, including the national public safety
24 broadband licensee, will provide practitioner-level
25 input to ERIC from the public safety community.

1 The third prong of the proposal concerns
2 funding. The plan assumes that where feasible public
3 safety can and should leverage commercial broadband
4 networks and technologies, which will substantially
5 reduce the cost of the network to public safety. The
6 plan also assumes that the broadband could piggybank
7 on existing infrastructure belonging to federal,
8 state, local, and tribal entities. In this regard,
9 the plan recommends that funds of about \$11.3 million
10 be provided to FEMA to survey and collect data on
11 state and local and tribal public safety broadband
12 deployment.

13 But we also know that reliance on commercial
14 networks and existing infrastructure alone will not
15 meet public safety specific needs for network
16 reliability, resiliency, and nationwide coverage that
17 includes remote as well as populated areas.
18 Therefore, the plan proposed specific public funding
19 for both capital expenditures and the network
20 operating costs.

21 The funding for capital expenditures is
22 projected in the plan at \$6.5 billion over 10 years,
23 which would be in the form of federal grants to public
24 safety. This would pay for the public safety radio
25 access portion of the network, hardening of existing

1 sites, and construction of additional sites where
2 needed, and caches of deployable equipment that could
3 be moved to the site of an emergency.

4 The plan also recommends \$6 to \$10 billion
5 in public funding over 10 years for operating expenses
6 to be paid for by a small monthly public safety fee
7 billed to all broadband users. The plan recommends
8 that the operating costs be funded because we
9 anticipate the public safety entities will continue to
10 need to operate their existing narrow band voice
11 systems for some time. So the broadband network will
12 effectively be a second network used mostly for data
13 during this period.

14 In slide two we list some of the key
15 benefits from the approach recommended by the plan.
16 It provides for a network that meets public safety's
17 requirements for reliability, enhanced performance,
18 and interoperability while enabling public safety to
19 benefit from commercial economies of scale that lower
20 its costs. This will benefit public safety not only
21 now but in the future by allowing public safety to
22 keep pace with new innovations as broadband technology
23 evolves.

24 In slide three we provide an illustration of
25 the variety of broadband resources that will be

1 available to public safety users under the
2 architecture proposed in the plan. Out the foundation
3 is the dedicated public safety network operating on
4 public safety's dedicated spectrum, which would
5 support the vast majority of public safety broadband
6 operations both day to day and in emergencies. The
7 public safety would also have access to other
8 resources as needed.

9 As mentioned previously, the plan provides
10 for roaming and priority access on commercial networks
11 when additional capacity is needed. The plan also
12 recommends taking steps to improve in-building and
13 underground coverage through the increased use of
14 distributed antenna systems and microcells.

15 And finally, the plan calls for funding to
16 purchase deployable equipment caches that can be moved
17 quickly to an emergency scene such as a remote area
18 lacking infrastructure or an area where existing
19 infrastructure has been damaged or destroyed.

20 That concludes the summary of the public
21 safety broadband network. And with that, I will turn
22 it back to Jennifer.

23 MS. MANNER: Okay. Thank you very much,
24 David. And I just wanted to remind folks, as David
25 said, the slides, which are a little hard to read here

1 in the room, are going to be available on our web
2 site, so you'll be able to download those.

3 And with that, I'd like to turn the floor
4 over to Lisa Fowlkes, who is another one of our deputy
5 bureau chiefs, and she is going to focus on the next
6 generation alerting recommendations.

7 MS. FOWLKES: Thank you, Jennifer. Good
8 morning everyone. Let's see if -- go to the slide.
9 Okay, great.

10 As many of you know, one of the FCC's
11 priorities has been to ensure that Americans can
12 receive emergency alerts over as many communications
13 technologies as possible. And basically, what this
14 means is that Americans should be able to receive any
15 type of emergency alert, whether it is a weather alert
16 or an alert about a terrorist attack or some type of
17 biochemical problem, wherever they are, whatever they
18 are doing.

19 So if a consumer sitting in front of the
20 television watching their favorite programming with
21 their family, they should be able to get an alert
22 through the television. If they're in their car
23 driving and they're listening to their radio, they
24 should be able to get an alert through -- over their
25 radio. If they're on the go, if they're shopping, in

1 the grocery store, or they're shopping at the shopping
2 mall, and they have got their cell phone, they should
3 be able to get an emergency alert over their cell
4 phone. And if they're surfing on the internet, as
5 many of us do, consumers should be able to get some
6 type of emergency alert over the internet as well.

7 Today, the emergency alert system, otherwise
8 known as the EAS, is the primary way that is available
9 for the President and other alert originators to send
10 out timely and accurate emergency alerts to the
11 public. In 2008, the Commission established rules for
12 the commercial mobile alert system, otherwise known as
13 the CMAS. The CMAS is going to allow consumers to be
14 able to receive alerts over their cell phones.

15 And as many of you know, FEMA has been
16 working on what they call an integrated public alert
17 and warning system, otherwise known as the IPAWS,
18 which at the end of the day the goal is to have that
19 system be able to allow alert originators to send
20 alerts over a multitude of different technologies,
21 whether it is broadcast, cable, satellite, radio, and
22 television, wire line, wireless, as well as the
23 internet.

24 The national broadband plan takes the next
25 step in this process by recommending two initiatives,

1 one for the Commission, one for the executive branch.
2 The first initiative was a recommendation that the
3 FCC initiate a comprehensive inquiry into all issues
4 associated with developing a multiplatform redundant
5 broadband-based next generation alerting system.

6 The idea would be to look at different
7 potential multiplatform technologies. How can we
8 leverage broadband technologies to send out emergency
9 alerts? So the inquiry would look at what
10 technologies are out there, what technologies are
11 being developed that can be utilized to send out
12 emergency alerts. It would also look at the alerting
13 systems that we already have, such as the EAS and the
14 CMAS, to see how can we leverage broadband
15 technologies to -- with respect to those systems.

16 The inquiry would also look at IPAWS
17 because, as I said, IPAWS -- the goal of IPAWS is to
18 be able to leverage different types of technologies,
19 different types of communications technologies to send
20 out emergency alerts. So one important question --
21 one thing that we want to make sure of is that IPAWS
22 is able to leverage these different technologies,
23 including broadband technologies.

24 We anticipate the inquiry, for example,
25 would look at the internet and how we can leverage the

1 internet to send out emergency alerts. And finally,
2 the inquiry would look at what are the needs of state,
3 tribal, and local governments in utilizing this type
4 of next generation alerting system, and what can not
5 just the FCC but its federal partners do to help
6 state, local, and tribal governments utilize this
7 system. And when I say federal partners, I mean FEMA,
8 National Weather Service, and other federal agencies
9 that have their hands in alerting issues.

10 And that brings me to the second
11 recommendation, which was that the executive branch
12 take action to clarify the responsibilities and roles
13 of agencies that are involved in alerting. As I just
14 mentioned, alerting is one of those issues where a lot
15 of federal agencies have their hands in it. The
16 primary agencies are the FCC, FEMA, National Weather
17 Service. And of course, whenever you have a multitude
18 of anybody involved in a particular issue or a
19 particular project, you have the potential for
20 different agencies not knowing who is doing what and
21 when. You have the potential for the American public
22 not knowing who they should come to if they have got a
23 question about alerting. Is it FEMA that handles
24 this? Is it the FCC? Is it National Weather Service?
25 Who does what and when?

1 And so the recommendation is that the
2 executive branch clarify those roles and
3 responsibilities, not just to the agencies involved,
4 but to the American public so they know who they are
5 supposed to go to depending on what alerting issue
6 that they have a question about; also to set
7 milestones, benchmarks, and other actions that the
8 federal agencies need to take to get to the point of
9 having a next generation alerting system.

10 In other words, getting from the point of
11 talking about a next generation alerting system and
12 developing plans about a next generation alerting
13 system and actually laying down some markers as to
14 what is supposed to be done, who is supposed to do it,
15 and when is it supposed to be done.

16 And finally, the recommendations for the
17 executive branch to also set up a system of
18 accountability to ensure that all of the agencies, all
19 of the federal agencies particularly, that have their
20 hand in alerting, that have responsibility for
21 alerting, are routinely communicating with each other,
22 coordinating with each other, and most importantly,
23 when the federal government speaks to the American
24 public about alerting, they're speaking with a
25 coordinated voice, as opposed to having different

1 agencies speaking with different voices.

2 As we move forward -- and we're planning to
3 start moving forward on some of these things this year
4 -- we're very excited about -- particularly this
5 inquiry. We're very excited about it. We're hoping
6 to get input from a lot of stakeholders. And when I
7 say we're starting to think about it, what I mean is
8 among various issues we're starting to think about how
9 to be creative in providing ways for stakeholders to
10 provide us input, even before we issue this inquiry.

11 So I would certainly encourage those of you
12 that have an interest in alerting issues to, when the
13 inquiry opens, file comments. But even before that,
14 you know, feel free to get in touch with me or my
15 team -- Tom Behrs is sitting over here, wave your
16 hand, Tom -- to get in touch with us, to share with us
17 your ideas on how we can get to this point of a next
18 generation alerting system that utilizes broadband
19 technologies. Thank you.

20 MS. MANNER: Thank you very much, Lisa. And
21 with that, we're going to turn the floor over to Jeff
22 Cohen, who is the senior legal counsel for the Public
23 Safety and Homeland Security Bureau. And Jeff is
24 going to focus on the recommendations regarding next
25 generation 911.

1 MR. COHEN: Thanks, Jennifer, and good
2 morning everyone. Okay. This morning I am going to
3 talk about the current status of 911 and what our
4 recommendations are concerning next generation 911.

5 Today, the nation's 911 system is based on
6 decades-old technology and has been upgraded over time
7 to accommodate wireless 911 calls and voice-over
8 internet protocol or VOIP 911 calls. Enhanced 911
9 services today enable the automatic transmission of an
10 911 caller's phone number and location to the 911
11 call-taker, known as the public safety answering
12 point, or PSAP.

13 Next generation 911 is the evolution of
14 today's voice and phone based 911 system to a
15 broadband and IP-based platform creating new 911
16 capabilities. So NG-911 will enable the transmission
17 of not just voice, but also text, photos, video, and
18 e-mails to PSAPs, and from a variety of new devices,
19 services, and applications.

20 NG-911 will also enhance the communications
21 between the PSAP and dispatchers to first responders
22 and hospitals, resulting in a more interoperable and
23 integrated response. Thus NG-911 will enable vast
24 improvements in the quality and speed of response, and
25 also provide equal levels of service to people with

1 disabilities and non-English speakers.

2 For example, the potential for sending
3 photos and videos to the PSAP will provide first
4 responders with eyewitness quality information.
5 Broadband will be the enabler to make it possible for
6 PSAPs to receive and send videos, images, medical
7 information, environmental sensor information, and a
8 host of other data through shared networks and
9 databases.

10 As the slide that is up there now shows, the
11 process of transitioning from the legacy 911 system to
12 next generation 911 has begun. Public safety and
13 industry standards organizations have arrived at a
14 consensus on the next generation 911 technical
15 architecture. The Department of Transportation -- and
16 I see Larry Flaherty is here representing that agency
17 -- has published a transition plan for next generation
18 911 migration. And a few states and localities have
19 begun deployment of NG-911, and there is at least one
20 live test of texting to 911 that is ongoing.

21 However, many in the public safety
22 community, including PSAPs, lack access to broadband
23 services. Further, inconsistent, overlapping, and
24 outdated state and federal regulations have hindered
25 NG-911 deployment. Also, existing grant programs are

1 uncoordinated and limited in scope.

2 So turning next to what our recommendations
3 are, the recommendations in the national broadband
4 plan for NG-911 are intended to foster a rapid
5 transition from today's analogue, voice-centric 911
6 system to a broadband-enabled, IP-based emergency
7 services model.

8 We begin with the recommendation that the
9 National Highway Traffic Safety Administration direct
10 a report that analyzes the cost of deploying NG-911 on
11 a nationwide basis. This report could then serve as a
12 resource for Congress to develop a coordinated,
13 targeted, long-term funding mechanism for NG-911
14 deployment, transition, and operation. To address the
15 regulatory barriers to next generation 911, we next
16 recommend that Congress consider establishing a
17 federal legal and regulatory framework for the
18 development and transition to next generation 911.

19 Many of the existing rules and regulations
20 were written before the technological capabilities of
21 NG-911 existed. The federal framework should remove
22 jurisdictional barriers and inconsistent legacy
23 regulations and provide legal mechanisms to ensure
24 efficient and accurate transmission of 911 caller
25 information to PSAPs and emergency response agencies.

1 We also recommend that Congress consider
2 steps to curtail state, tribal, and local use of 911
3 funds for purposes other than 911. Further, we
4 suggest that Congress consider amending and
5 reauthorizing the enhanced 911 act and restoring the
6 E-911 implementation coordination office with
7 appropriate funding to potentially administer a new
8 NG-911 grant program and help ensure that NG-911 is
9 deployed in an interoperable and reliable fashion.

10 Our last recommendations concern actions the
11 FCC should take. And the two that I am going
12 recommend or mention are recommendations that would
13 take place this calendar year. First, the FCC should
14 build upon an existing proceeding, examining location
15 accuracy and automatic location identification
16 requirements for wireless and interconnected VOIP
17 services, to explore the impact of NG-911 on these
18 issues.

19 Second, the FCC should issue a notice of
20 inquiry to explore how public expectations may evolve
21 as new broadband and IP-based communication services,
22 devices, applications, and technologies develop, and
23 how deployment of NG-911 can meet these expectations
24 and accommodate new forms of communication.

25 That concludes my presentation. Thanks very

1 much.

2 MS. MANNER: Thank you very much, Jeff. I'd
3 next like to turn the floor over to Jeff Goldthorp,
4 who is chief of the bureau's communications systems
5 analysis division, and he is going to focus his
6 remarks on the cyber security recommendations. Jeff.

7 MR. GOLDTHORP: Thanks, Jennifer. And let
8 me add my welcome and thanks for being here today.

9 The national broadband plan has given the
10 Commission an opportunity to clarify its role in cyber
11 security. It's an area where we frankly don't have
12 much of a track record over the years, and we're
13 looking to establish more of a role in this area going
14 forward. And hopefully, you'll agree that the
15 recommendations that we have in the plan go a long way
16 towards putting us on the path to doing just that.

17 Let me first give you the framework for the
18 recommendations. There is two categories for the
19 recommendations that we have. There is one
20 recommendation that is more of a strategic
21 recommendation, trying to chart out a path for where
22 we think we should be going. I'll talk for a little
23 bit about that in a moment.

24 There is this other set of recommendations
25 that are more tactical in nature, that are more

1 focused on tasks, things that we can be doing. Now
2 they are based on a platform of things that we do
3 today, and we think that they are going fairly well.
4 But they need to be expanded or changed or modified in
5 some way. So I will talk about each of those in turn.

6 Let me talk first, though, about these more
7 strategic recommendations. We're recommending that
8 the Commission develop a cyber security roadmap to
9 examine or to identify the five most critical cyber
10 security threats facing the communications
11 infrastructure, as well as end users that rely on that
12 communications infrastructure, things that we in
13 coordination with our federal partners and other
14 stakeholders can accomplish in the next two years.

15 We're looking to get that done in the next
16 180 days. It's a tall order, but we are fortunate
17 that a lot of the work to identify -- I'm okay without
18 the slides -- we have the advantage that a lot of the
19 work to identify these issues have been done -- has
20 been done already. So a lot of the issues and the
21 threats have been identified now. We will be using
22 some of that work. We'll be coordinating with the
23 executive branch as well to identify the threats and
24 identify what we should be doing to deal with them.
25 So that's the roadmap.

1 Now let me turn to the more tactical items.
2 And as I said before, these are based on the platform
3 of things that we do today to deal with communications
4 infrastructure reliability and security. We have a
5 set of rules on the books. Part 4 of our rules deals
6 with outage reporting of legacy, traditional
7 communications infrastructure. For example, we get
8 reports when there is larger fiber cuts. We get
9 reports when switches go out service. When a certain
10 number of customers are affected for a certain amount
11 of time, we get outage reports from wireless and wire
12 line carriers. When signaling systems, legacy
13 signaling systems, are out of service, we get a report
14 here.

15 We get a lot of data from this. We get
16 maybe 30, 40 outage reports a day. Over time -- and
17 it doesn't take much time, frankly -- we can rack up
18 statistically significant analyses of this data. We
19 can work then with individual communications providers
20 and with the industry at large to try and improve
21 things. So we use this data in a process of
22 continuous improvement to reliability and security.

23 The reporting requirements themselves are
24 mandatory. The work that we do with the
25 communications industry once the data comes in is

1 voluntary. But it is surprising how powerful data is
2 when data is presented in way that is, as I said
3 before, statistically significant. And so that is our
4 network outage reporting system. The weakness that we
5 see in that system today is that we get no data on
6 internet service providers or interconnected VOIP
7 providers. And we're recommending in the plan that
8 that gap be closed, that our information collection
9 regime be extended to embrace those technologies and
10 services. That way we can apply the same types of
11 techniques with that segment of the industry to
12 instantiate improvements over time.

13 We also have a system in place that they
14 call the disaster information reporting system, DIRS.
15 This is a voluntary system that we activate in
16 emergencies. We do it in collaboration with FEMA and
17 with DHS, the NCS. It has only been activated a few
18 times since we put it into place in 2000 -- I want to
19 say 2006. It might have been 2007 when we actually
20 designed it and deployed it.

21 But it isn't activated much. As I say, it's
22 voluntary. It's more asset-based. So in the disaster
23 or the affected area, we are asking for information
24 about assets that are affected by the event, switches
25 that are down or on backup power, cell sites down or

1 on backup power, backhaul connections that are severed
2 for one reason or another. And that information is
3 provided daily. Unlike the network outage reporting
4 system data, which is provided over a longer period of
5 time, the DIRS data comes to us every day. We share
6 it just like with NORs, by the way. We share it with
7 DHS and NCS. It goes to FEMA as well and is used in
8 the disaster area to help in the recovery and the
9 restoration efforts that are going on in that area.

10 This is a system that, just like NORs, is
11 limited to legacy and existing communications systems.
12 So existing public switch telephone network systems,
13 wireless systems, and so forth. High capacity
14 transport pipes are all part of the infrastructure
15 that we get in DIRS. We don't get anything on cyber
16 attacks in DIRS on the communications infrastructure.
17 And to the best of our knowledge, information that
18 crosses the industry about cyber attacks on
19 communications infrastructure doesn't exist right now.

20 We're recommending that the DIRS model be
21 extended to a system called the cyber security
22 information reporting system so that that gap can be
23 closed as well. As with DIRS, we would share that
24 information in real time with DHS, with NCS, maybe
25 with the national cyber security division. It may be

1 the more applicable entity there. But that's yet to
2 be determined. We would develop it in coordination
3 with DHS, so the data model would be developed in
4 coordination with DHS as well as with stakeholders
5 that are involved in submitting the data. That's
6 exactly how the DIRS data model was developed.

7 The final recommendation that we made in the
8 plan has its basis in the best practices that we have
9 developed over the years in our federal advisory
10 committees. The Network Reliability and
11 Interoperability Council developed a long list of
12 cyber security best practices. Some of the most
13 detailed and specific, and frankly some of the best,
14 best practices that we have are the cyber security
15 best practices.

16 We are recommending in the plan that we put
17 forth a certification regime so that communications
18 providers can come to us and request that they be
19 granted certification subject to a process that is yet
20 to be determined, and a set of criteria that while
21 possibly based on the best practices would not be
22 checklist-based. And there is a very important
23 distinction there. We don't perceive or we don't
24 expect that the certification regime that we have in
25 mind would be, quote, "checklist-based." It would be

1 more aimed at instantiating or implementing a culture
2 of cyber security and the entity that we are doing
3 certification for.

4 So those are the recommendations for cyber
5 security in the plan. Thanks for your attention, and
6 I'll turn it back over to Jennifer.

7 MS. MANNER: Thanks so much, Jeff. And with
8 that, I'd like to turn the floor over to John Healy,
9 who is a communications systems specialist in the
10 communications systems analysis division. And John is
11 going to focus his remarks on the critical
12 infrastructure recommendations. John.

13 MR. HEALY: Excuse me. The critical
14 infrastructure recommendations actually come in three
15 parts. First, we're going to be issuing a notice of
16 inquiry on current broadband network survivability.
17 We're also going to be working on developing broadband
18 priority services. And the third one is related to
19 developing standards for broadband network
20 reliability. I'll be discussing each of these items
21 in the next two slides. Can I have the first slide up
22 now?

23 The first critical infrastructure
24 recommendation is to issue a notice of inquiry on
25 broadband network survivability in April. It's going

1 to be covering the resilience of broadband networks to
2 physical failures, whether these failures are caused
3 maliciously or non-maliciously. When Jeff was talking
4 about the cyber security stuff, that is generally a
5 malicious type of failure.

6 Our primary goal here is going to be to
7 assess how well broadband networks, including
8 broadband access networks, can withstand direct
9 attacks or direct failures. We have a good
10 understanding of what happens with current networks
11 because of what Jeff was talking about with the
12 network outage reporting system. But we really don't
13 have a really good understanding of what happens in
14 broadband networks. What are the major single points
15 of failure?

16 So in this notice of inquiry, we'll be
17 asking about the major single points of failure in
18 broadband networks. Essentially, these are the
19 physical places in the network that if they fail, you
20 will have a major loss of broadband service. We're
21 going to be asking about what measures communications
22 providers already do to minimize single points of
23 failure.

24 In addition, we are going to be looking into
25 the ability of redundancy that is in place to actually

1 function properly. There was an outage just recently
2 in Washington, D.C. It was in the PSAP. There was a
3 power failure, and they had a backup system. It was a
4 backup generator, and the backup generator was not
5 able to be brought online. Essentially, the transfer
6 switch did not function. This is a failure of -- this
7 is an example of redundancy not acting properly.

8 So we're also interested in the ability --
9 in what the FCC can do to improve the resiliency and
10 the survivability of broadband networks, particularly
11 when emergency services ride these broadband networks.
12 Again, one of the major reasons why we're interested
13 in broadband reliability is because we anticipate and
14 we know that public service networks are all going to
15 be migrating to broadband, and emergency service
16 networks will also be migrating to broadband.

17 The NOI will also look into the ability of
18 broadband networks to withstand severe overloads.
19 these overloads could be caused by pandemics,
20 bioterrorism, but probably more often they will be
21 caused by natural disasters like hurricanes and maybe
22 earthquakes, or whatever. Current telecommunications
23 networks have lots of network management controls in
24 place to handle overloads. However, we are not sure
25 exactly what kinds of management controls are in place

1 for broadband networks, particularly when we
2 transition these broadband networks to public safety.

3 So how susceptible are these networks to
4 severe overloads, and how adequate current network
5 management techniques to handle these overloads?
6 These are the types of questions that we're going to
7 be having in this notice of inquiry.

8 Finally, since there is no equivalent of
9 wireless priority service on broadband networks, we're
10 also going to be asking for information on the need
11 for priority services during severe overloads.

12 Okay. My second viewgraph actually gets
13 into the next two parts. And when we're talking about
14 priority services, this first major bullet really
15 addresses the priority services. As you probably
16 know, the FCC and the national communications systems
17 have been deeply involved in priority services over
18 the years, and lots of other agencies and companies
19 have been involved in these priority services. These
20 services have been in place for wire line, traditional
21 wire line, and wireless networks. These include the
22 Government Emergency Telecommunications Service, GETS,
23 and the Wireless Priority Service, WPS.

24 We plan to use our experience in jointly
25 developing a system of priority network access and

1 traffic routing for national security and emergency
2 preparedness users on broadband communications
3 networks. Basically, we want to extend what we know
4 for our current networks to broadband networks.

5 We will probably -- and we're planning on
6 getting the executive branch involved to help us
7 delineate the various responsibilities and help the
8 FCC and the NCS actually move this process along. It
9 actually took a fair amount of time to actually get
10 some of the priority services implemented, like
11 wireless priority service. We're actually hoping that
12 we can get broadband priority services implemented in
13 a quicker fashion.

14 The final recommendation is related to
15 extending what we learned from the first NOI. This
16 bullet is entitled "broadband communications
17 reliability and resiliency." Essentially, this is
18 trying to determine what types of standards should be
19 in place for broadband network services, particularly
20 broadband network services on networks that handle
21 public safety and handle emergency services.

22 So the idea here is we want to get explicit
23 and implicit standards for reliability and resiliency.
24 So what should these standards be? Should these
25 standards be at what level? Should they be just at

1 the physical level, or should they be at higher
2 network levels, at the service level? We're
3 interested in what the role of the FCC should be in
4 establishing these standards or ensuring that these
5 various networks actually meet these standards.

6 So both these NOIs will ask questions about
7 the recommended role of the FCC in ensuring
8 reliability of broadband networks. I'd like to stress
9 that it is really critical that broadband networks
10 have very high reliability, particularly since public
11 safety and emergency services will be riding these
12 networks in the future.

13 So thank you for your attention, and I'd
14 like to turn it back over to Jennifer.

15 MS. MANNER: Thank you so much, John. And
16 with that, what I would like to do is ask Ken Moran,
17 who is the senior deputy bureau chief in the Public
18 Safety and Homeland Security Bureau, to talk about two
19 issues. He is actually going to cover Project Roll
20 Call and the Stafford Act. Ken.

21 MR. MORAN: Thank you, Jennifer, and thank
22 you all for coming. During a major disaster, the FCC
23 works with its federal partners, FEMA, the National
24 Communications System, NTIA, and others in assisting
25 and restoring critical communications systems and

1 services. Our focus is on first responders, state,
2 local, and tribal emergency operation centers, 911
3 centers, wire line and wireless telecom systems -- he
4 wireless cellular systems are especially important
5 during these disasters -- broadcasters who provide
6 essential emergency information such as when, where,
7 and how to evacuate, location of food and water
8 supplies, and emergency healthcare facilities.

9 During a disaster, one of the FCC's first
10 roles is determining which essential communications
11 systems are working and which are not, and this can be
12 very difficult to determine because often our standard
13 way of contacting these parties is through the
14 telephone, and the telephones aren't working, or
15 perhaps the personnel are unable to reach their
16 facilities to respond.

17 So basically, shortly after Katrina, we
18 designed and assembled some devices, which we called
19 Project Roll Call units. They're made up of
20 receivers, spectrum analyzers, and computers, and
21 these roll call units do a number of sweeps through a
22 wide range of spectrum. They take RF power readings.
23 They organize the information in files, and they use
24 software to associate the spectrum information to the
25 FCC's licensees. And from this, we are able to

1 determine what spectrum is in use and who the spectrum
2 licensees are. And we can tell whether the police
3 department is having communication problems, whether
4 the fire departments are having communication
5 problems. In short, which first responders are having
6 problems, which state, local, and tribal emergency
7 operation centers are having problems, which
8 broadcasters are having problems. And this
9 information is summarized quickly and reports that are
10 provided to the federal emergency communications
11 leadership and staff on the ground, generally led by
12 FEMA, and these roll call reports help FEMA establish
13 priorities and allocate limited federal resources in
14 restoring the most essential communications systems
15 first.

16 So where are we on the Project Roll Call?
17 We have five fully operational roll call packages. We
18 have one cellular unit. These cellular systems
19 architecture don't allow the standard roll call units
20 to work well for them, so we've acquired a cellular
21 package also. We also have access to a number of
22 remote fixed monitoring sites throughout certain parts
23 of the country that help us in this regard. And this
24 whole program is managed by the Public Safety and
25 Homeland Security Bureau, and also staffed by the FCC,

1 although the bureau -- also the field personnel and
2 enforcement bureau also work on the project.

3 The Project Roll Call units have become very
4 much in demand and an integral part of the federal
5 emergency communications response. And as a result,
6 we are working continually to try to improve the
7 system. We are working to improve the accuracy and
8 speed of reporting, the capability of the cellular
9 units. And we want to acquire more of those units.
10 We are training FCC field engineers throughout the
11 country, with the help of FEMA, so that our field
12 agents around the country will be able to operate this
13 equipment.

14 One of the things we are doing on a day to
15 day basis is we will bring these roll call units into
16 an area and turn it on, get reports to try to get an
17 RF footprint of how -- of what the area looks like
18 under normal operating conditions. We will store all
19 that information, and if sometime in the future a
20 disaster occurs in that information, we'll run the
21 roll call unit out, turn it on after the disaster
22 occurs. So we will have sort of a pre-disaster, post-
23 disaster data. We will compare the data, and this
24 actually helps us get more accurate determinations of
25 who should be up and doesn't appear to be operating,

1 and who may be up at less than full capacity. So we
2 are continually working on that.

3 For the broadband aspects of this, however,
4 as the broadband plan is implemented, we will need to
5 develop or procure new roll call units that provide
6 rapid detection for the public safety and first
7 responders that are going to be operating on the 700
8 megahertz range. These units will have to be also
9 upgraded. The roll call units will have to be
10 upgraded or redesigned to be useful in assessing
11 operation of broadband applications. And we'll also
12 -- we believe we need a lot more of these units.
13 We're going to acquire a number of them and put them
14 in various parts of the country, so if something
15 happens, a disaster happens, we will be able to get
16 these systems up and running and get the information
17 we need to the federal responders and try to help
18 resolve them.

19 This, of course, will take a lot of money.
20 We've got estimated capital costs of I think something
21 like \$7 million with annual operating costs of
22 something like \$2 million once the broadband plan is
23 fully operational.

24 So I guess in summary on the roll call,
25 these roll call units have been shown to be very

1 effective to help the federal and FCC emergency
2 communications response to disasters, but it is very
3 clear that we're going to have to make additional
4 investments in these units to make them useful as the
5 broadband plan is rolled out.

6 So that concludes my remarks regarding the
7 broadband -- the roll call project. And I guess the
8 next project -- the next issue is the Stafford Act.
9 Okay. Federal support during disasters is governed by
10 the Stafford Act. And under the Stafford Act, federal
11 entities, including the FCC, cannot provide direct
12 support to for-profit entities. And this can present
13 major challenges to us because for-profit entities own
14 and operate probably between 80 and 90 percent of all
15 of the nation's critical communications
16 infrastructure, and most of it is broadcast
17 facilities, for example.

18 So consider this situation, why this can
19 present real problems for us. A non-English
20 broadcaster goes out of service during a major
21 disaster in a metropolitan area, and it is the only
22 Spanish language broadcaster in the area. As a
23 result, Spanish-speaking listeners do not receive
24 understandable EAS messages. They do not receive
25 information on where, when, how to evacuate. They do

1 not receive information on when, where, and how to
2 find food, water, and essential medical treatment.
3 They do not receive information on what to do if there
4 is an electric power line down in their neighborhood.
5 They don't receive information as to what to do if
6 there is a gas leak in their home.

7 As troubling as this may be, these are real
8 world situations. We have run across them in Katrina
9 and in some situations since then. So today, the FCC
10 and its federal partners, primarily FEMA, try to solve
11 these non-English language broadcaster problems
12 through liaison activities. These activities are
13 slow, they are indirect, and quite often they are
14 unreliable. So in the national broadband plan, we are
15 asking the Congress to consider changes in the
16 Stafford Act so that for-profit entities that provide
17 essential communications services can be provided
18 direct federal support.

19 The FCC Katrina panel report and the
20 chairman's 30-day public safety review made similar
21 recommendations. This would allow FCC and our federal
22 partners to take more direct steps to keep such
23 broadcasters in service or to restore operations more
24 rapidly by providing perhaps emergency power
25 generators, fuel, and other equipment. So we think it

1 is real important, and the broadband plan makes that
2 recommendation.

3 That concludes my comments on the Stafford
4 Act.

5 MS. MANNER: Thank you very much, Ken. And
6 with that, our last speaker is Brian Hurley, who is an
7 attorney advisor on the policy division in the Public
8 Safety Bureau.

9 MR. HURLEY: Thank you, Jennifer. Our final
10 recommendation is to ensure that broadband satellite
11 service is a part of any emergency preparedness
12 program. Both fixed and mobile satellite can provide
13 a communications option and critical source of
14 redundancy for public safety, and it may be especially
15 important during the early stages of a disaster, when
16 terrestrial-based services may be damaged or
17 destroyed.

18 Already, several state, local, and federal
19 agencies use satellite services for public health,
20 continuity of government, and disaster preparedness,
21 and our plan is to build upon these efforts. In
22 particular, the plan proposes that federal agencies
23 recommend the use of broadband fixed and mobile
24 satellite service for emergency preparedness and
25 response as well as for national security, homeland

1 security, continuity, and crisis management. Thank
2 you.

3 MS. MANNER: Thank you very much, Brian.
4 And before I open the floor to questions, I just
5 wanted to introduce also Erika Olsen, who is joining
6 us, who is at the end of the panel. She is our legal
7 advisor in the bureau.

8 So with that, I'd like to open the floor for
9 questions. But I would ask folks to identify
10 themselves, please. Do we have any questions? Do you
11 want to go up to the microphone here? Thanks, Harold.

12 MR. SALTERS: Oh, figure out how to work
13 this. There we go, much better. Thanks, Jennifer.
14 Harold Salters, T-Mobile. A question for Jeff about
15 C-I-R-S versus -- Jeff Goldthorp. We talk to each
16 other so much it's just Jeff. C-I-R-S versus D-I-R-S.
17 You have got D-I-R-S as being an event-driven
18 reporting system. Do you envision CIRS being event
19 driven, or is it a situation/when-it-happens?

20 MR. GOLDTHORP: Well, I'm trying to -- I'm
21 not sure if I -- I think I know what the question is.

22 MR. SALTERS: Oh, I mean an event being an
23 externally-generated event, such as occurs with DIRS.

24 MR. GOLDTHORP: Yeah.

25 MR. SALTERS: Now there have been, for

1 instance, cyber attacks that have been discussed. Is
2 that the kind of event that would trigger CIRS? Or is
3 CIRS just an ongoing --

4 MR. GOLDTHORP: Yeah, all right. Now I
5 understand your question. If it could be done, if it
6 was technically feasible to have CIRS, or C-I-R-S,
7 activated only during what would you would describe as
8 an event, you know, an event that would be worthy of
9 activating it, then that's how it would be done. If
10 it was possible to do something like that technically.

11 But now with -- we're not dealing in the
12 same kind of environment that we were with DIRS, where
13 you have got -- with DIRS, the most frequent things we
14 were activating DIRS were for hurricanes, where you
15 had days -- you know, we knew days in advance there
16 was a hurricane approaching the coast. Or most of the
17 things that DIRS gets activated for take some time to
18 develop, and we have some time to prepare and to
19 activate.

20 With CIRS, it is a much more fast-moving
21 environment. Events are just sort of overtaking
22 themselves in real time by the millisecond. So it's
23 hard for me to imagine sitting here right now how a
24 system like that could work if it wasn't -- if there
25 wasn't some situational awareness all the time of what

1 was happening. So maybe it would be some -- I'm
2 thinking out loud right now. But you can imagine some
3 sort of a cold CIRS or a version of CIRS that is just
4 sort of in monitor mode, until it sees something that
5 rises to a threshold that would say, okay, we really
6 do need to look much more closely at this.

7 The thing that CIRS would be used for is
8 information sharing in an environment in which that
9 sharing of information would be helpful. So that's
10 what -- you know, I mean, you want to make sure the
11 information is there when that activation happens,
12 when people need it. So that's why I'm sort of
13 stumbling towards an answer to your question. I don't
14 have the specific answer. But I can't think of a way
15 that we could do it right now where it would just be
16 off until it's on. It's not going to be binary like
17 that. All right?

18 MR. SALTERS: Okay. Thank you.

19 MS. MANNER: Thank you, Harold. Does anyone
20 else have any questions? Please step up to the
21 microphone, sir.

22 MR. BELL: Lisa -- Frank Bell -- three
23 questions. What consideration has been given to
24 applying digital TV and HD radio as an optional
25 feature, not a mandate, to improve EAS using consumer

1 receivers? Second question --

2 MS. MANNER: Maybe -- do you want to take
3 them one at a time, Lisa? Is that easier?

4 MR. BELL: Well, is it -- okay. I've got
5 three.

6 MS. FOWLKES: What has been -- I'm just
7 trying to make sure I understand the question. What
8 has been --

9 MR. BELL: What consideration has there been
10 given to enabling there to be an optional feature for
11 digital TV receivers and HD radios to improve EAS
12 beyond the present analogue system?

13 MS. FOWLKES: Well, the FCC a few years back
14 adopted rules that extended EAS to digital television
15 and to digital radio. Beyond that, I am not aware of
16 any other -- I mean, beyond that, I am not aware of
17 any additional action that the Commission has taken on
18 that particular issue. But what the FCC has been
19 focused on in the past with EAS is basically expanding
20 it. So as broadcast, cable -- and you now get these
21 satellite radio and TV, which were already digital by
22 nature -- as those have developed, to basically adopt
23 rules that make it clear that in addition to all the
24 analogue stuff, the EAS now also applies to the
25 digital aspect of those systems.

1 MR. BELL: Okay. Anyway, just to clarify
2 that question, I was meaning in terms of applying
3 newer technology, not replicating analogue functions.

4 Second question. Would the redundancy and
5 cost effectiveness of sending, for instance, CAP
6 messages over digital broadcasters be desirable as a
7 part of improving EAS within IPAWS as an improved EAS
8 system?

9 MS. FOWLKES: I think as you and I talked
10 before the meeting, we have recently issued a public
11 notice that talks about part 11 and changes taken into
12 account the introduction of CAP by FEMA. To the
13 extent people raised that in response to that public
14 notice, that might certainly be something that we
15 might consider looking at.

16 MR. BELL: Okay. Last question. Has a
17 market research assessment been made of current and
18 proposed future alerting technologies to help
19 elucidate known unknowns, for example, the value and
20 compared with the annoyance, of relevant compared with
21 irrelevant, alerting message types?

22 MS. FOWLKES: To my knowledge, no such
23 research has been done. But, you know, that might be
24 something that the Commission might want to consider
25 looking at in the context of the inquiry that I

1 mentioned. So, you know, good questions, good ideas.
2 I would, you know, suggest that -- you know, the
3 second question you asked, that might be something to
4 raise in the context of the public notice regarding
5 CAP EAS. And the second question, that might be
6 something, you know, for us to consider in the context
7 of the inquiry looking at next generation alerting.

8 MR. BELL: Thank you. I don't know if
9 anyone else wants to respond to any of those.

10 MS. MANNER: Yeah. Thank you so much. Are
11 there any other questions for the panelists? You're a
12 quiet bunch. Okay. With that then, I'd like to thank
13 everyone here today for participating in the broadband
14 plan. I think this marks an important time for the
15 Commission, where we go ahead in implementing things
16 as quickly as possible. As our panelists discussed, I
17 think I counted anywhere from 12 to 20 proceedings
18 potentially that will have to be addressed in the
19 coming months. And I think that means a lot of us
20 continuing to work very closely with all of you, and
21 we look very much forward to it. Thank you again.

22 (Whereupon, at 10:35 a.m., the colloquium in
23 the above-entitled matter was concluded.)

24 //

25 //

REPORTER'S CERTIFICATE

CASE TITLE: Colloquium on the Public Safety and
Homeland Security Portion of the
National Broadband Plan

HEARING DATE: March 31, 2010

LOCATION: Washington, D.C.

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

Date: March 31, 2010

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

Heritage Reporting Corporation

(202) 628-4888