James Arden Barnett, Jr., Rear Admiral (Ret.)

Chief, Public Safety & Homeland Security Bureau

Federal Communications Commission

Communications Sector Coordinating Council

April 7, 2010

Washington, DC

Thank you for the opportunity to speak with you today. I'd also like to thank Robert Mayer, for the invitation to be here and for his work as chair of the Communications Sector Coordinating Council. It's a privilege to be here.

I think this is a great and timely opportunity to share with you the details of the National Broadband Plan's recommendations for advancing public safety and homeland security. Our recommendations set forth in the Plan are the culmination of a year-long process and draw upon a substantial record. Many of the organizations represented here have contributed to that record through your active participation in this process. Your input has been very influential in shaping the recommendations I will discuss today, and I thank you for your efforts.

However, our work has just begun. It will take a tremendous effort over the ensuing months and years to implement the Plan's recommendations, and I look forward to working with you throughout that process as well.

Is there anyone here who hasn’t heard about the *Comcast v. FCC* decision yesterday? We're still assessing the implications of the *Comcast* decision and remain firmly committed to achieving the policy goals articulated in the National Broadband Plan.

--with respect to protecting emergency communications and our nations cybersecurity, we are focused in particular on questions around:

--ensuring that the FCC has adequate information about outages of IP-based communications

--guaranteeing that users of IP-based communications services (like texting, IP to IP VOIP, and Next Generation handheld devices) have access to 911 and related services during emergencies

--developing best practices for cybersecurity protections by commercial Broadband providers, and

--establishing standards and best practices to ensure that commercial IP networks are capable of surviving natural and manmade disasters.

So we are pressing ahead with the National Broadband Plan even as we assess *Comcast.*

The public safety portion of the National Broadband Plan covers a lot of ground. The part that has received perhaps the most attention is our comprehensive strategy for creating a nationwide public safety broadband network. That strategy includes an administrative system for ensuring that public safety users have sufficient capacity and access to commercial technologies at reasonable rates; the creation of an Emergency Response Interoperability Center to ensure nationwide interoperability and operability of the network; and a request for public funding to support the network's construction and operation. In addition, the Plan includes proposals for accelerating the development of Next-Generation 911, and for promoting next-generation alerting.

The Plan also includes several recommendations for improving cyber security and securing our nation's critical infrastructure, and these will be the focus of my remarks today.

It is clear that the Nation faces tremendous challenges in cyberspace – from crime to espionage to outright sabotage. Accordingly, our first recommendation in this area is for the FCC, in coordination with the Executive Branch, to identify, and to develop a roadmap for confronting our nation's five most pressing cyber security threats. The roadmap should establish a two-year plan, with milestones for addressing each threat. Ultimately, the goal is to produce a clear strategy for securing the communications networks on which public safety and critical infrastructure users both rely.

To assist us in accomplishing this goal, I invite your input on these issues. What are our nation's most pressing cyber security threats and how should we address them? Also, what milestones should we set? Your views on these questions would be very helpful to us in developing our roadmap. I should note, however, that we are working within a very short time-frame; therefore, we will need your input within the next few weeks. I recognize that this is not a lot of time, but we are moving quickly to meet the

Plan’s recommendation that the roadmap be completed within 180 days of the Plan’s release. I thank you in advance for your help on this very important issue.

Another one of the Plan’s recommendations is that the Commission start a proceeding to look into extending the FCC’s Part 4 outage reporting requirements to broadband ISPs and interconnected VoIP providers. I realize that some of the organizations represented here have expressed concern over this proposal, but we believe the information that would result from this proceeding is essential to improving our understanding of broadband service outages, how to respond to them when they occur, and how to prevent them in the future. I would also note that we are open to new ways of acquiring this information, and the rulemaking will give us an opportunity to explore these.

The Plan also recommends establishing a voluntary cyber security certification program and exploring whether other voluntary incentives are appropriate. An FCC proceeding will soon be underway to seek comment on the development of this program. We invite your participation in this process as well.

Another cyber security recommendation is to develop a Cyber Security Information reporting system (CIRS) to accompany the existing Disaster Information Reporting System (DIRS). CIRS would serve as a real-time monitoring system for cyber events affecting the communications infrastructure and would allow for rapid dissemination of information during such events. Finally, the plan recommends that the FCC expand its international participation and outreach on cyber issues.

On critical infrastructure survivability, the plan recommends two inquiry proceedings, one to address network preparedness and resilience, the other to address standards for reliability and resiliency of broadband communications. The Plan also recommends the creation of a priority network access and routing system for broadband communications. I look forward to working with you on all of these issues.

Thank you for having me here today to talk with you about these very important matters. Your cooperation and input on these issues is extremely important to us as we move forward in developing new and innovative ways to improve public safety communications and cyber security across the nation.

I’ll be happy to take any questions you have.