Introductory Remarks
Commissioner Meredith Attwell Baker
Cyber Security and Broadband Workshop
September 30, 2009

Good morning. I would like to welcome everyone to the Cyber Security and Broadband Workshop. I am happy to have the opportunity to kick off this important event, and I thank you all for being here today.

Broadband has become critical infrastructure – the enabling technology for everything from the future of our children's education, the next generation of health care, smart energy grid development, and public safety. According to one metric, the communications industry constitutes one-sixth of our economy and is the foundation upon which the rest of it runs. A 21st Century communications infrastructure is essential for restoring sustained economic growth, opportunity, and prosperity.

The Commission will play an important role in making sure that the right regulatory environment exists to create incentives for companies to build out infrastructure faster, to reward innovation and investment, and to encourage competition so that American consumers have access to, and can afford, the world's most advanced communications services.

However, as society grows ever more dependent on broadband and as traditional platforms are increasingly open and interconnected with the Internet, we become more susceptible to cyber security threats. In fact, the number of security breaches on computer and communications systems increases daily.

Because the potential for harm to communications systems due to cyber attacks is so immense, I firmly believe that network security is one of the most important issues facing the communications industry. Consumers expect and need reliable and secure broadband infrastructure to distribute information, to do banking, and to make investments and everyday purchases. Most sectors of our economy routinely rely on the durability and security of IP-enabled communications networks to securely collect and move large quantities of data, and broadband systems are also a critical component of our national defense and emergency preparedness.

Attacks on communications infrastructure can result in severe harm, ranging from identity theft and the disclosure of sensitive and proprietary information to service degradation and disruption for all users, including public safety entities. Cyber security is crucial to ensure confidence in the use of any network – whether wired or wireless – and, without such confidence, we lose a significant foundation of our economy and homeland security capabilities. If we do not get it right, it could derail all of our other broadband plans.

So, the Commission has a part to play in ensuring that our communications infrastructure is secure, and I am pleased that we are continuing to focus on the importance of cyber security. To this end, the Commission is already engaged in reviewing its own needs and reaching out to industry and other government agencies to address network security issues and enhance our awareness and ability to respond to cyber attacks. I would like to take a few minutes to acknowledge some of our activities in the cyber security area.

Cyber security is not only an issue for the companies that we regulate, but also for the Commission itself. I applaud Chairman Genachowski's initiative in ordering a 30-day review of the Commission's Preparedness for Major Public Emergencies. This review, which the Chairman announced almost immediately after being sworn in, resulted in a report, issued earlier this month, that discusses, among other things, the ability of the FCC to prevent, monitor, detect, and analyze cyber attacks and recommends areas in which improvements can be made. I encourage the Commission to institute procedures to protect and respond to attacks on its own networks. Hopefully, we can lead by example.

I am also encouraged by the creation of the Commission's inter-Bureau Cyber Security Working Group to evaluate our role in network security, assess the needs and requirements for cyber security expertise and assets, and identify vulnerabilities. This Working Group will deliver a report to the Chairman by the end of November with specific recommendations to address deficiencies.

We should also continue to engage with industry to develop best practices to secure networks against intrusions. The Commission has taken positive steps in the past by chartering and working closely with the Network Reliability and Interoperability Council (NRIC), a Federal Advisory Committee composed of private sector representatives established to develop best practices for ensuring reliability and resiliency in telecommunications networks. NRIC issued an extensive series of more than 200 industry best practices aimed at improving network security.

This work will be continued by the Communications Security, Reliability, and Interoperability Council, which was recently re-chartered to review and update the cyber security best practices to take into account new and advanced technologies including broadband and IP-based technologies. The Commission is also providing outreach and education to encourage implementation of cyber security measures. We should continue to collaborate with and assist industry to develop the tools and technologies to protect infrastructure and restore and recover networks after cyber attacks.

The Commission should also pursue policies that foster innovation and investment in security technologies for communications networks and have procedures in place to aid industry members and the public safety community to recover from network intrusions.

Congress has instructed the Commission to develop and implement a National Broadband Plan. By February 17, 2010, we must and will deliver to Congress a Plan that seeks to ensure that every American has access to broadband capability and establishes clear benchmarks for meeting that goal. In formulating this Plan, we need to consider how to secure broadband networks.

The Commission is off to a good start by requesting comment on public safety and homeland security concerns – and specifically on cyber security. Over the past several weeks, we have held numerous workshops on a variety of topics to assist in the creation of the National Broadband Plan. Today, we look to the public safety community, government agencies, academia, and industry to provide their expertise on the important topic of cyber security. These two panels will discuss the ability to prevent, detect, and respond to attacks and consider how broadband technologies, tools, and innovations can assist efforts to secure the nation's critical communications infrastructure.

That said, I would like to introduce Admiral Jamie Barnett, the tremendously capable Chief of the FCC's Public Safety and Homeland Security Bureau, who will introduce and moderate the first panel.