Remarks of
Michael K. Powell
Chairman, Federal Communications Commission
At the
NSTAC XXVII EXECUTIVE SESSION LUNCHEON
U.S. Chamber of Commerce
May 19, 2004
Washington, D.C.
(as prepared for delivery)

Good afternoon, and thank you for allowing me the opportunity to address the Executive Session of the National Security Telecommunications Advisory Committee. I particularly want to thank Dr. Vance Coffman for his efforts in arranging this lunch, and bringing together such a distinguished group of industry leaders.

It is indeed a pleasure to be here, for we share a desire and a commitment to provide the American public with the most secure, competitive, and technologically advanced telecommunications infrastructures possible.

Security in an Expanding Communications Universe:

When President Ronald Reagan created the NSTAC in 1982, he was seeking ongoing advice on the pressing telecommunications security issues of the day, primarily the breakup of AT&T and the increasing dependence of the government on private telecommunications infrastructure and services.

Over the past 20 years, we have seen a vibrant, dynamic, and competitive telecommunications market develop. Today's communications market offers Americans unprecedented choices, and the number of innovative communications platforms continues to expand at a remarkable rate.

As economic and consumer welfare grows from the expanding communications universe, so too, does our dependency on critical communication networks. Moreover, the task of securing the multiple and varied networks on which our knowledge economy rides becomes more challenging. In the post 9/11 world, security is our greatest challenge and must be our highest priority. Just as we have embraced economic policies that advance new platforms and new competition, we must embrace the responsibility of expanding our security focus to encompass all relevant components of the ever-changing communications cosmos.

The challenges are complicated not just by the ever changing nature of the communications landscape, but also by the fact that the threat to our national security is far more complex than that of a generation ago. The Cold War presented enormous, even catastrophic risks to the world; but the nature of that risk possessed a clarity not found in today's edition of evil – terrorism involves a foe that is far more fragmented,

diffuse and elusive – and with terrorism, threats morph constantly and are difficult to identify and neutralize.

I am convinced, however, that with industry and government standing shoulder to shoulder we can protect the network and our nation. The Commission has worked hard with the industries in our sector to advance the mission of making our communications systems secure, reliable and resilient. Furthermore, we must be proactive and scout the emergence of future technologies to ensure that we incorporate a security focus into them as they unfold. I know NSTAC is equally committed to these critical objectives.

Homeland Security:

We are well aware of the weight of the challenge, but I am buoyed by the opportunities. The FCC has set out to deeply integrate a homeland security focus into our operations as well as drive industry to adopt critical practices.

First, give me a moment to summarize our effort to make security an integrated component of sound communications policy. I have made homeland security one of the six pillars of the Commission's Strategic Plan, and each of the Commission's Bureaus and Offices has integrated a homeland security focus into its work. Our goal is to provide leadership in evaluating and strengthening the Nation's communications infrastructure and to facilitate rapid restoration in the event of disruption.

To achieve our goals we need to work across all platforms and to step outside our traditional "stovepipes". In order to facilitate this new thinking, we created a Homeland Security Policy Council comprised of senior management from each of the Bureaus and Offices to develop and coordinate the Commission's Homeland Security initiatives. In addition we opened an Office of Homeland Security, dedicated to this mission.

Let me now turn to our efforts to work with industry to harden our networks and plan for contingencies in case of disruption. The Network Reliability and Interoperability Council, has a long tradition of developing industry practices to prevent and plan for network outages on the wireline phone network.

In 2002, we re-chartered NRIC to address the new and urgent threat to our homeland. Both its focus and membership were broadened, recognizing the need to take a more holistic view of network security. Specifically, the composition of NRIC VI was expanded beyond wireline carriers to include wireless carriers, ISPs, the satellite industry and others. By the end of 2003, NRIC VI, under the very capable chairmanship of Richard Notebaert of QWEST, had revised over 800 best practices to better prepare operators of the public switched telecommunications network, and to address emerging issues of cyber-security. The FCC has taken steps to promote the adoption of these best practices, producing, for example, a DVD tutorial that we have distributed to over 600 carriers and other interested parties.

A few months ago, we raised the curtain on NRIC VII, asking it to focus more sharply on wireless network issues. Reflecting that focus, NRIC is chaired by a member of the wireless industry for the first time – taking command is Timothy Donahue, President and Chief Executive Officer (CEO) of Nextel Communications Inc. An area of special attention will be how to drive ubiquitous Enhanced 911 deployment for wireless services. Ensuring that public health and safety personnel have effective communications services available to them in emergency situations is vital, and furthering the deployment of new technologies that enhance Homeland Security has been a centerpiece of our agenda. The prominence of wireless issues in NRIC itself reflects the rapid growth of communications platform alternatives for voice service.

September 11th highlighted the importance of redoubling our efforts on wireline and wireless, but it also revealed the critical need to do something to prepare and better utilize our media networks. Consequently, the Media Security and Reliability Council was literally "born" of the 9/11 tragedy. On September 11, with the destruction of the World Trade Center, 22 New York City broadcasters lost their transmission facilities, and over-the-air broadcast service was disrupted to the largest market in the country. In the immediate aftermath, suffering both a loss of technical facilities and the personal loss of staff who died on the roof of the World Trade Center, these New York City broadcasters were inventive in finding alternate distribution facilities.

MSRC was created to institutionalize and expand on the response to that experience. More broadly, its goals are to study, develop and report on best practices designed to assure the optimal reliability, robustness and security of the broadcast and multichannel video programming and distribution industries.

The group brings together representatives from across the media industry. In its first years, it was chaired by Dennis J. FitzSimons, CEO of the Tribune Company. It adopted over 100 best practices designed to ensure the continuous operation and security of media facilities, and to operationalize mutual assistance in times of emergency.

These best practices cover such diverse topics as local coordination and planning, emergency procedures, EAS, vulnerability assessments, disaster recovery plans, physical security, and redundant facilities. In December of 2003, in conjunction with the Florida Association of Broadcasters, we actually conducted a "model city" project in Tampa, Florida to test these best practices. Over 100 participants attended, including officials from DHS, FEMA, the Florida State Cable Association, local Florida Broadcasters, and local emergency managers. This type of exercise is essential. If you don't test and practice your plan, you don't have a plan.

MSRC was recently rechartered, and in the next two years, under the leadership of David Barrett, CEO, Hearst/Argyle, it will focus on fostering coordination among local emergency managers and media. The first meeting is on June 2, when we will also host a forum with DHS and other governmental and private entities on the role of media in Homeland Security.

In addition to MSRC and NRIC, with other federal partners, we have undertaken or expedited initiatives that will enhance government-wide communication capabilities in the event of an emergency. These initiatives include the Wireless Priority Access System, which allows officials in high-risk locations to communicate with each other more reliably in a crisis, and the Telecommunications Service Priority System, which, as you know permits priority restoration of government and private wireline systems that are critical to swift recovery from an incident.

We also continue to work with our colleagues at state regulatory agencies to ensure the continued security and robustness of our telecommunications infrastructure. In June we will be holding a "Critical Infrastructure Inter-dependency Workshop" in coordination with NARUC's Ad Hoc Committee on Critical Infrastructure, the Department of Homeland Security and the Federal Energy Regulatory Commission. At this forum, federal and state entities involved in critical infrastructure protection and homeland security will address the interdependence among energy, water and telecommunications services.

The FCC also allocates and manages spectrum, which, in the Homeland Security arena, has led us to conduct rulemakings and other proceedings aimed at providing public safety entities the spectrum and technologies they need to function in today's world: the 800 MHz proceeding, the 4.9 GHz proceeding; our narrowbanding proceeding; and proceedings enhancing technological developments with clear Homeland Security implications such as RF ID Tags and the ground penetrating capabilities of UWB are just a few examples.

New Technologies/Convergence:

At the same time that we are taking steps to ensure the security of our telecommunications networks and infrastructure, we are turning a corner on the digital migration. Innovative entrepreneurs are replacing yesterday's slow, limited networks with many different types of high-speed, full-service digital networks, such as BPL, WIFI, FTTH, Cable Modem and DSL. And these networks are ushering in the latest advanced applications, like internet voice, streaming video and music services. Competition among these facilities-based networks, combined with the openness of Internet Protocol, has begun to introduce the transformative forces of innovation and entrepreneurial spirit into a sluggish telecommunications sector. While this new age brings tremendous promise and opportunity, it also carries new risks. Again, first and foremost among those challenges is security.

There are incredible opportunities presented by a converged world, both for Homeland Security and consumer choice. Robustness is built into the very fabric of packet networks like the Internet. On September 11 one of the Internet's most important metropolitan hubs, New York City, suffered extensive physical damage – communications equipment and fiber optic cables at ground zero were damaged or disabled by the attack. The effect on Internet services was primarily localized. Packets, like water flowing toward a downhill destination, are tenacious in seeking out alternate

paths. As the National Academy of Sciences reported, the September 11 attack had minimal impact on the Internet as a whole and the network displayed great flexibility in the face of extreme stress.

IP-enabled services, like voice over the internet, undoubtedly present challenges, but we should focus as much on the promise as the problems. Consider, as an example, 911 service. When a person in distress calls 911 today, he reaches an operator in a dispatch center who, often only receives a call-back number and a location. All other information comes from the often-distressed caller. Imagine a world where technology could do more. Imagine that chronically ill people are equipped with wireless devices that could transmit their critical vital signs to dispatch centers. Imagine wireless devices embedded in vehicles that could transmit the nature of the accident – for example, if it involved a rollover – to the dispatch center. Imagine a dispatch center that could send this, and countless other, critical scraps of intelligence to emergency personnel. Imagine how many lives would be saved. Keeping the world unchanged is not a virtue, making it better is.

Already today, two percent of U.S. firms use some form of IP telephony, and that number is expected to grow to 19 percent by 2007. A new Yankee Group survey found that 73 percent of wire line service providers and 31 percent of wireless operators either have implemented, or were testing, packet telephony in their networks.

As a regulator, the FCC is embracing the reality that the torrent of change from IP technologies has arrived, is unstoppable and will accelerate over the coming years. And American citizens will be the richer for it. A critical aspect of our job is to establish regulation that allows the ever-changing telecommunications industry to flourish. If we do not create a regulatory climate that attracts and encourages investment, we will face the rude realities that opportunity can and will go elsewhere. The President has set forth a bold vision of ubiquitous broadband connectivity by 2007 – creating a friendly regulatory environment for the deployment of these services is a priority of the highest order for this Commission.

But to bring this discussion full circle, one cannot expect to enjoy the fruits of progress, if you do not ensure those who wish you ill cannot easily snatch it from you. A critical aspect of our job is to ensure that our security focus expands as the telecommunications universe expands. That is a job for ALL of us. We have a historic opportunity to build security into our evolving network at the front end of its development, rather than trying to bolt things on at the end. We should not let it pass us by.

Conclusion:

Industry/government partnerships are the key. The NSTAC is a model for such partnership. Together we should pair our enthusiasm for new technological advances with an enthusiasm for securing them. I look forward to continuing our work together. Thank you.