Telecommunications Security: Key Issues Affecting the Public and Private Sectors

Seventh Annual Midwestern Telecommunications Conference
Remarks of Commissioner Kathleen Q. Abernathy
April 2, 2004

Thank you very much for giving me the opportunity to talk to you about telecommunications security issues. I am sorry I was unable to make the trip to Marquette, my alma mater, but thanks to modern technology I can offer these remarks from Washington, D.C.

The challenges associated with ensuring secure and reliable telecommunications networks have always been important issues for industry and regulators alike. And after 9-11, our focus on these issues has intensified. We used to worry about things like earthquakes and ice storms, and perhaps teenage computer hackers, but terrorism was not a major concern. Of course, 9-11 changed all of that — it propelled security issues into the forefront of our work and our lives.

Well before 9-11, the FCC had chartered what is now called the Network Reliability and Interoperability Council, or NRIC. This body is made up of top telecom executives, and its focus is developing best practices to minimize service outages and ensure that networks remain up and running in crisis situations. These standards rely on the principles of redundancy and interconnectivity so that knocking out a single piece of the network should not impair service on a broad scale. After 9-11, the FCC reinvigorated the NRIC process and focused more directly on responding to security threats, in addition to traditional reliability concerns. NRIC finalized its homeland security best practices last year, and I understand that carriers are implementing these new procedures.

The public-private model exemplified by NRIC also has been extended to other sectors. NRIC itself has recently been rechartered and is currently focusing on public safety and emergency services. In addition, the FCC chartered a related body called the Media Security and Reliability Council, or MSRC, to ensure that the radio and television industries are equipped to deal with security threats. These bodies are premised on the belief that voluntary industry processes can do a great deal to promote security and reliability. Some argue that regulatory mandates are necessary, but I believe that we should always explore cooperative approaches and best practices before leaping to the conclusion that heavy-handed regulation would work better. In fact, in my experience a more cooperative model typically produces better results.

Even if we do not adopt regulatory mandates, government has a critical role to play and needs to work together at all levels —federal, state, and local. At the FCC, in the wake of 9-11, Chairman Powell established a Homeland Security Policy Council to coordinate the FCC's activities with other governmental entities, such as FEMA, the Office of Science Technology Policy, the National Communications System, and more recently the Department of Homeland Security. Last year, the FCC created a new Office of Homeland Security, which supports our Policy Council and also assumed other functions. For example, our Homeland Security Office operates a 24-hour Communications and Crisis Management System and works closely with our Managing Director's Office on our Continuity of Operations Plans.

The FCC is also working with state regulatory commissions on security and reliability issues. I represent the FCC on an ad hoc Critical Infrastructure Committee formed by NARUC — the National Association of Public Utility Commissioners. This group brings together state and federal officials to discuss how to safeguard public utilities and related issues. The Committee is currently planning a forum with the Department of Homeland Security, the FCC, and FERC to consider interdependencies in our telecom, energy, and other utility infrastructures.

Finally, in addition to sponsoring industry collaboratives and participating in inter-governmental coordination, the FCC has made telecom security part of its policy agenda in recent years. For example, the FCC recently adopted a notice of proposed rulemaking seeking comment on modifications of our network outage reporting requirements that apply to traditional telecom providers, and the possible extension of such obligations to wireless carriers, satellite operators, and providers of cable telephony. While I am always cautious when it comes to extending new regulatory requirements to competitive industries, our compelling interest in network security made it necessary to launch this proceeding.

In the wireless arena, the FCC has focused on security and related issues in many different contexts. For example, the FCC has implemented a priority access system to ensure that government officials can get access to the network during emergencies. The FCC also has aggressively promoted the deployment of E911 in wireless networks to make sure that a customer's location and call-back information are available to public safety answering points. In addition, the FCC has undertaken several initiatives to identify additional wireless spectrum for use by public safety officials, which would help promote interoperability among police and fire departments and other emergency responders. And we are conducting an important proceeding right now to prevent interference to public safety communications caused by commercial services in adjacent bands.

In the wireline context, the FCC recently revised its rules concerning the universal service subsidy mechanism for rural health care clinics, and one of our primary objectives in doing so was to ensure that regional hospitals and rural clinics are interconnected in the event of a bioterrorism incident. More generally, the FCC's ongoing rulemakings on broadband services and voice over IP have focused on security issues — something that probably would not have occurred before 9-11.

Lastly, in the satellite arena, the FCC has worked to ensure recognition of the homeland security role that satellites play across other industries, adding satellite companies to both NRIC and MSRC's membership. We have also worked to improve E-911 capabilities of mobile satellite service systems and highlighted the homeland security and public safety applications of satellites in rural areas.

As this very brief overview illustrates, security issues have become pervasive in the field of telecommunications. As a regulator, I have focused my remarks on some of the initiatives undertaken by the FCC and other agencies, but we all must take responsibility for improving security and reliability. I know that the companies you all represent take this very seriously, and I urge you to continue to make it a top priority.