TESTIMONY

TESTIMONY OF

Joseph P. Nacchio
Chairman & Chief Executive Officer
Qwest Communications International, Inc.

Before the Senate Governmental Affairs Committee

October 4, 2001

CRITICAL INFRASTRUCTURE PROTECTION: WHO IS IN CHARGE?

Good morning, Mr. Chairman and Members of the Committee. It is an honor to be here this morning to share Qwest's views on this subject of paramount national importance. Thank you for holding this timely hearing and for including us among these distinguished panelists. Let me begin by briefly introducing my company and myself.

Qwest is a four-year old Fortune 100 company, with 66,000 employees and annual revenues of over $20 billion. We are a telecommunications company of the 21st century, providing local and long distance, telephone, wireless, and Internet web hosting services over a state-of-the-art network to homes, businesses, and government agencies in the United States and around the world, including the US Departments of Defense, Energy, and Treasury.

Although I am here today in my capacity as Chairman and CEO of Qwest, I also serve as Vice Chair of the National Security Telecommunications Advisory Committee, often referred to as NSTAC. NSTAC is an organization of 30 CEOs from the telecommunications, technology and other industries who share information about emergency preparedness and advise the President and other White House leaders on a wide range of national security and related concerns. I bring to this organization, and to the Committee today, my thirty years' experience in the telecommunications industry, particularly on issues relating to information security and critical infrastructure protection.

Mr. Chairman, two weeks ago the President reassured the nation that the state of the Union is strong. This morning I offer you the same assurance regarding the nation's telecommunications infrastructure. America's telecommunications infrastructure is the best in the world, and the engineers, technicians, and workers who maintain it are second to none in their technical ability and selfless dedication. We saw the proof on September 11. Despite the horrific damage sustained at the World Trade Center and at the Pentagon, the nation's telecommunications infrastructure continued to operate. It brought us the sounds and images of tragedy, it summoned emergency rescue services, and it alerted our military forces.

At Ground Zero in New York, telecommunications companies put aside

their everyday marketplace rivalry and came together as one to help restore communications in lower Manhattan. For example, Qwest immediately diverted a multimillion-dollar shipment of switching equipment to lower Manhattan, gave top priority to any and all requests from emergency service providers engaged in rescue and recovery efforts, and provided free Internet connections and services to those who had lost them. Similar efforts were made by many other telecom companies -- a collaborative industry undertaking praised by FCC Chairman Michael Powell as "heroic efforts…insuring that the world's premier communications network has continued to be available in this time of tragedy."

I stress this point because, where some have focused on how *vulnerable* our networks are, we must also remember how *resilient* they are. In this sense, our networks' performance during and after this indelible national tragedy can teach us some valuable lessons about the control and protection of critical infrastructures that the Committee is asking this morning.

First and foremost, the telecom industry understands that our networks are, quite literally, the conduit that connects the other essential sectors of our economy. For that reason, we understand that we bear a unique responsibility in being the first line of defense in protecting our own infrastructure. Keeping both our *internal* and *external* networks safe is something that companies in the telecom industry do every day — and will continue to do in the future.

Let me give you two examples of this from our own experience. First, to defend our *internal networks* from both physical and cyberattack, Qwest has implemented a comprehensive information network security program, which includes classification of network assets, the development, implementation and monitoring of a complete set of security policies and procedures, extensive employee training, and a plan for disaster response and recovery. Qwest's security program serves as a model for other companies, and will shortly be recommended for adoption by all NSTAC industry members. Second, to protect our *external networks*, just last month Qwest dedicated more than 1,000 technical experts to assist our customers affected by the global "Code Red" computer virus. Such a quick and comprehensive response to threats to network operations has become a necessity.

But, in all candor, it's not enough. Other industries need to take similar steps to protect their own critical infrastructures. Communications providers know from experience that any network is only as strong as its weakest link, and we can only protect communications networks up to the point of service. Vulnerable infrastructure in any industry affects all~~other~~ industries. A communications provider can have the most secure network in the world, but if other industries we serve have vulnerable infrastructures, our networks may continue to be open to attack. In other words, *each* company must therefore protect *its* own critical infrastructure; and *all* companies, whether managing and operating critical infrastructure or running traditional business operations, have a responsibility to exercise prudent risk management.
Private sector companies are in charge of protecting their corporate assets, including digital data and networks, physical facilities, and people. Officers and directors have a fiduciary duty to their shareholders to protect corporate assets and operations. This means they must take security of their data and networks seriously. Quite simply, corporate America must begin to exercise oversight, effectively manage

infrastructure risks, institute corporate security plans, adequately fund security initiatives, and look for ways to collaborate on critical infrastructure protection.

The public sector and its agencies have additional responsibilities as well. I'll briefly mention three. First, as in business itself, a major aspect of communications network design is risk management. When designing a network, agency mission and objectives are calibrated to reflect the acceptable level of risk. As of September 11, the definition of acceptable risk was dramatically changed, and such concepts as the need for redundancy, single point of failure, and the reliability of a network now need to be redefined.

Second, increased standardization of security requirements across the agencies is crucial. Terms like "redundancy," "single point of failure," and "reliability" need to be precisely and uniformly defined. Presently, agencies interpret these terms differently and leave it to the vendors to attempt to discern their intent. Also, with "lowest cost" evaluation models the government often inadvertently encourages vendors to shortchange security requirements to minimize their bids and then perhaps "evolve" their proposals to deal with the technical security issues after contract award. Obviously, such an approach leads to no consistency across the government in its ability to resist or respond to network attacks. Standardization cries out for attention.

Finally, the Government must take steps to increase the sharing of information. During the recent crisis, the efforts of NSTAC and the National Coordination Center demonstrated that one of the best means to defend against terrorists is the timely and accurate sharing of information. Private sector companies should not be subject to FOIA requests or other exposure from the Government, investors or competitors for helping to protect critical infrastructure. Appropriate legislation should be crafted to protect companies similar to the legislation that was developed for the Y2K problem.

This brings me to the issue of how companies and the public sector can jump-start their efforts in the face of this national emergency. Here again, the telecommunications industry's longstanding history of shared responsibility and cooperation provides a model to follow.

NSTAC has been key in furthering shared industry responsibility and private-public sector cooperation. In terms of facilitating interindustry efforts, NSTAC studied Qwest's internal network security program, and has recommended that all its member companies adopt it to safeguard their own networks. And during the unfolding tragedies on September 11 NSTAC's National Coordinating Center and its Information and Analysis Center for Telecommunications operations, supported by many of our members, played a pivotal coordinating role in restoring telecommunications services and providing essential communication needs in both New York City and at the Pentagon.

How can we best build on the current framework to broaden its scope and increase its effectiveness? There are several interrelated ways of doing this. For example, NSTAC and the National Security Council should immediately initiate a project to develop benchmarks and requirements for Information Security Best Practices for the telecommunications industry. Either NSTAC or a public organization, such as the National Infrastructure Simulation and Analysis Center proposed by Senator Domenici, could be given the responsibility to extend these clearinghouse

and coordination functions to other industry segments as well.

No matter what organizational structure you establish to carry out these expanded planning and coordination functions, it will not succeed if existing law works against the ability of companies and government to freely share sensitive information on infrastructure protection. Legislation introduced recently by Senators Bennett and Kyl recognizes this. Congress should remove real or perceived barriers to information sharing in order to allow the exchange of critical information about infrastructure threats and assure that the information exchanged will not, directly or indirectly, fall into the hands of our enemies. And Congress should complement these efforts by enacting legislation increasing the penalties for cyberattacks and acts of vandalism that impair the telecommunications infrastructure, and by giving law enforcement greater latitude to investigate and prosecute these attacks.

I'm a businessman, not a lawyer, so I won't presume to advise you about the privacy and other legal ramifications of the information sharing and wiretapping legislation Congress is now considering. But as a telecom executive I can assure you that our networks are sound and ready to help preserve our national security.

Conclusion

In my testimony I have stressed several points: *first*, telecommunications companies have a critical responsibility to defend their internal and external networks against physical and cyberattack, and to adopt policies and procedures that will do this; *second*, all companies must strive to ensure the security of their data and networks; *third*, interindustry coordination and industry/government cooperation are essential to these efforts; and *fourth*, there are a number of steps that Congress should take to enable these efforts to be both broader and more effective.

And now let me conclude. I began by saying that our country's telecommunications infrastructure is strong — and it is. But it can, and must, be stronger. I speak for Qwest, and without doubt for the rest of our industry, when I commit to you that we will do whatever is necessary to work with this Committee and the Congress to assure the continued strength of the networks that make up America's telecommunications infrastructure.

Committee Members | Subcommittees | Hearings | Key Legislation | Jurisdiction
Press Statements | Current Issues | Video of Select Hearings | Sites of Interest