NEWS

Federal Communications Commission
445 12th Street, S.W.
Washington, D. C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC. 515 F 2d 385 (D.C. Circ 1974).

For Immediate Release
December 6, 2002

News Media Contacts:
FCC: Robin Pence (202) 418-0505
Qwest: Vince Hancock (303) 965-6950

HOMELAND SECURITY: COMMUNICATIONS INDUSTRY CONSIDERS MEASURES TO PROTECT NATION'S COMMUNICATIONS SERVICES AGAINST ATTACK

Washington, D.C. – Representatives from across the communications industry came together today to consider recommendations to protect and strengthen the nation's communications infrastructure against terrorist attacks or national disasters.

The measures were considered by the Network Reliability and Interoperability Council (NRIC) VI which held its quarterly meeting today at the FCC. NRIC is composed of representatives from the telecommunications, cable, wireless, satellite and ISP industries.

The 56-member Council will review some 300 best practices – many of which are currently being practiced by industry members – for widespread adoption and implementation across the industry. Best practices range from increasing physical security at communications facilities to process changes and training to increased protection of proprietary information. NRIC members have until December 20, 2002 to vote on recommendations to the industry that these best practices voluntarily be implemented.

FCC Chairman Michael Powell said, "Homeland Security is a critical issue that touches every consumer in America. People want to know that in an emergency their calls will go through and they can reach loved ones. Every bit as important, our nation's communications network must be secure and protected to ensure that public safety, health, and law enforcement officials are able to respond and ensure the flow of information."

Richard C. Notebaert, NRIC chairman and chairman and CEO of Qwest Communications International, said, "Today's meeting illustrates the industry commitment to work together and share best practices in an effort to improve network reliability and strengthen the nation's communications network against terrorist attacks and natural disasters."

"The telecommunications industry has taken a leadership role in proactively identifying and protecting our nation's communications infrastructure. Many of the best practices we have heard today are actively being implemented by many companies. I strongly urge the industry to adopt as many of these Best Practices as appropriate to ensure the protection and reliability of our nation's communications system," Powell continued.

In developing its best practices, NRIC's Physical Security Focus Group, led by Karl Rauscher, director, network reliability office, Lucent Technologies Bell Labs, and NRIC's Cyber Security Focus Group, led by Dr. Bill Hancock**,** vice president, Cable & Wireless, underwent a rigorous process that included a detailed vulnerability and threat assessment and identified the best practices currently in use by the industry to take necessary steps to improve security and mitigate associated risks.

The items considered today include:

Best Practices for Securing the Physical Network:

- Technology. Best practices for the application of new technologies to better mitigate the effects of an attack.

- Access Controls. Best practices for access control methods and procedures to help ensure that unauthorized personnel do not have access to critical network infrastructures. Best practices include the development of formal procedures for assigning facility access and constructing physical barriers to prevent vehicular and pedestrian "tailgating," electronic surveillance at critical access points and changes to landscaping and outdoor lighting.

- Personnel. Best practices for security procedures and associated training including recognizing and reporting suspicious items and handling of proprietary information.

- Design and Construction. Best practices for new network and facility design and construction methods to help secure critical infrastructure.

- Inventory Management. Best practices and procedures for managing critical inventory to hasten restoration of service in the event of an attack. This includes best practices to establish procedures, including storage, handling, transfer and transmission.

- Auditing and Surveillance. Best practices for measuring and assessing security readiness in a communications firm, including physical inspection of equipment, network and software and plant locations.

- Elevate Internal Role of Security. Best practices to elevate security as an integral part of strategic business planning.

Best Practices for Securing the Cyber Network:

- Technology . Best practices for secure cyber technologies and architectures.

- Operations and Administrative. Best practices to help secure network information and operations support systems. The Focus Group's recommendations covered areas such as authentication and logging of network management actions, special access controls for network operations systems, and secure, swift distribution of operations system patches.

- Authentication and Access Control. Best practices for access control methods, policies and procedures to help ensure that only authorized personnel have access to critical network elements and information systems.

- Incident Management. Best practices for identifying, reporting, surviving and responding to cyber attacks.

- Users. Best practices for protecting public communications networks against attacks from end-user networks.

NRIC VI will recommend adopting voluntary outage reporting for cable, wireless, data and ISP service providers. The trial will commence on January 1, 2003 and conclude on December 31, 2003 and provide valuable information to improve the reliability of these networks.

NRIC, which has been in place since 1992, has a long history of providing the industry with a collaborative forum for developing and voluntarily implementing best practices. Earlier this year, NRIC VI adopted an Emergency Assistant Agreement which provides the means by which industry carriers and service providers can elect to enter agreements to collaborate to restore service in the wake of an emergency. It also adopted industry emergency contact procedures and protocol to provide detailed contact information, procedures and protocol to members in times of emergency and to identify communications industry representatives who are essential to effective communications and Internet service restoration efforts.

Chairman Powell chartered NRIC VI January 7, 2002 to focus on homeland security by ensuring the security and sustainability of public telecommunications networks in the event of a terrorist attack or national disaster. Membership in NRIC was significantly expanded through NRIC VI to include corporate representatives from the cable, wireless, satellite and ISP industries. It also established four new working groups to address homeland security: Physical Security, Cyber Security, Disaster Recovery and Public Safety.

-FCC-