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
March 14, 2003

NEWS MEDIA CONTACTS
FCC: Robin Pence (202) 418-0505
Qwest: Vince Hancock (303) 965-6950

HOMELAND SECURITY: COMMUNICATIONS INDUSTRY CONSIDERS MEASURES TO PROVIDE SERVICE CONTINUITY AND DISASTER RECOVERY IN THE EVENT OF ATTACK

Washington, D.C. – Leaders from the telecommunications, ISP, satellite and cable industries today began consideration of widespread recommendations to help restore communications services in the event of an attack on the nation's communications infrastructure.

The recommendations were presented by members of the Network Reliability and Interoperability Council (NRIC) VI at its quarterly meeting today at the FCC. The 56-member Council will review more than 200 best practices – many of which are currently being practiced within the industry today – for adoption and implementation. Votes will be completed on March 28, 2003.

FCC Chairman Michael Powell said, "Today's meeting marks the end of the first phase of NRIC's mission to develop best practices that will help fortify our industry's critical infrastructure and secure communications for all Americans. Our work is just beginning and much will be asked of us in the months ahead. The industry must now act to adopt and implement these recommendations to ensure the viability and operations of our communications services."

Richard C. Notebaert, NRIC chairman and chairman and CEO of Qwest Communications International, said, "The communications industry continues to prove its willingness to review and adopt the appropriate best practices so that industry players can continue to raise the bar on the performance and reliability of communications products and services. The communications industry takes its role in homeland security very seriously and this work effort demonstrates this commitment."

In developing its best practices for service continuity and disaster recovery, industry representatives identified and analyzed more than 200 best practices, covering a wide range of scenarios. In the area of cyber security, this represents the first time the communications industry has conducted a thorough assessment and analysis of best practices.

Emergency Preparedness/Disaster Recovery

In addition to the more than 300 best practices to protect communications networks that were adopted by NRIC in December, the Disaster Recovery/Business Continuity Focus Group, led by Gordon Barber,general manager, staff, Bell South, and Joseph Tumulo, director business continuity planning, Verizon, presented some 70 best practices the industry should consider to help sustain critical business activities in a crisis. These recommendations include, but are not limited to:

- Designate and brief key personnel
- Develop emergency management procedures
- Establish a remote alternative emergency operations center
- Conduct practice drills of emergency procedures
- Secure alternative power supplies
- Back up critical systems, information and internal communications
- Diversify critical business infrastructures

Service Restoration/Recovery Procedures

In the event a network is attacked, the Cyber Security Focus Group, led by Dr. Bill Hancock, vice president of security and chief security officer, Cable and Wireless, and the Physical Security Focus Group, led by Karl Rauscher, director, network reliability office, Lucent Technologies Bell Labs, identified more than 200 best practices the industry should consider to restore service in a timely and secure manner.

General best practices include, but are not limited to:

- Develop processes or plans to quickly account for all employees in or near the impact area of a disaster
- Rapidly assess the situation and execute immediate action steps designed to contain the problem and limit further damage
- Secure the physical perimeter of the breached area
- Isolate systems that pose an immediate threat to external entities or critical business functions (e.g. removal of an Ethernet cable or phone line or logical isolation through the use of firewalls and routers).
- Rebuild from a trusted media source

- Change all system passwords and examine relationships with hosts for signs of compromise

- Use forensic and post-mortem analysis techniques to develop a complete understanding of the event for future preparedness

- Increase network surveillance following an intrusion

- Train appropriate personnel (e.g. shipping and receiving, mailroom, emergency response and security personnel) to be aware of possible secondary events immediately after an incident and promptly report any suspicious conditions

- Enact the Mutual Aid Agreement with industry partners to aid in service restoration

Phase I Deliverables Complete

With today's presentation, NRIC VI has completed its Phase I homeland security deliverables to identify best practices to protect the nation's communications infrastructure against attack and to prepare for service continuation and disaster recovery should an attack occur.

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. In 2002, NRIC VI adopted a Mutual Aid 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. In December, the Council voted on some 300 best practices to protect the nation's communications against attack.

Phase II: Industry Outreach and Implementation

With the completion of its Phase I best practices deliverables, NRIC VI now moves into Phase II that focuses on adoption and implementation of these best practices. The FCC, working closely with industry will soon launch an aggressive education and awareness campaign with the goal of securing widespread industry adoption of those best practices that are relevant to respective businesses.

NRIC VI's Charter

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 -