WRITTEN STATEMENT

of

KENNETH P. MORAN
Director, Office of Homeland Security
Enforcement Bureau
Federal Communications Commission

Before the
Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
United States House of Representatives

On

"CyberSecurity: Protecting America's Critical Infrastructure, Economy & Consumers"

September 13, 2006

Good morning, Mr. Chairman and distinguished members of the Subcommittee. My name is Ken Moran and I serve as the Director of the Federal Communications Commission's Office of Homeland Security. In that role, I am primarily responsible for coordinating the Commission's emergency preparedness and critical infrastructure protection efforts. Specifically, my role is to help the Commission: (1) strengthen measures for protecting the Nation's critical communications infrastructure; (2) facilitate its rapid restoration during disasters; and (3) ensure the Nation's emergency responders have access to effective communications services at all times.

In my testimony today, I will describe advisory councils, such as the Network Reliability and Interoperability Council (NRIC) and the Media Security and Reliability Council (MSRC) that the Commission uses to promote highly reliable and rapidly restorable communications systems for the Nation, including the Internet. Then, I will describe some of NRIC's cyber-security best practices. Finally, I will review the lessons the Commission has learned during last year's catastrophic storms.

The Importance of Communications in Times of Disaster

The September 11, 2001, terrorist acts and last year's devastating hurricanes starkly illustrate the need for reliable communications during emergencies. During 9/11, for example, first responders and medical personnel were alerted of the tragic events by a range of telecommunications platforms, including pagers, cellular telephones, wireline telephones, and the Internet. Long distance communications, including satellite telecommunications, were used to initiate the movement of equipment and personnel into the affected areas for restoration purposes. All levels of government coordinated their restoration and homeland defense efforts through wireless and wireline phones, Internet networks, and pagers. After Hurricane Katrina and Rita, when communications infrastructures had been destroyed or impaired, the absence of

familiar methods of communication severely hampered the relief and recovery effort. Clearly, the need for immediate, secure, and reliable communications services is no more obvious than during a large-scale disaster.

As more and more traffic on the public telecommunications network migrates to Internet-based technologies, the importance of these technologies and the services they can bring to the public safety and homeland security community grows in proportion. As this migration proceeds, the well-understood and secure environment of the existing switched telephone network will be overtaken by the vastly more complex environment of Internet-based communications. Today's public networks, while complex, have the benefit of being nearly closed systems to which only a few trusted individuals have access. This makes security relatively easy to manage. On the other hand, Internet-based communications systems are de-centralized and use open systems; as a result, there are substantial challenges to prevent cyber attacks and to ensure their overall reliability.

The Network Reliability and Interoperability Council

In 1992, the Commission established the Network Reliability and Interoperability Council (NRIC) in accordance with the provisions of the Federal Advisory Committee Act. The Nation had experienced a series of major service outages in various local exchange and inter-exchange telephone networks, and the Commission established the NRIC to study the causes of service outages and to develop recommendations to reduce their number and their effects on consumers.

The first NRIC consisted of CEO-level representatives from carriers, equipment manufacturers, state regulators, and large and small consumers. Under its initial charter, NRIC commissioned studies in the areas in which the Council believed reliability concerns to be

greatest – network signaling, cable cuts, switching system failures, power failures, fires, 911 outages, and digital cross-connect systems. The Council's analysis led to the development of nearly 300 Best Practices and other recommendations, most of which, though formally presented to the Commission, were intended to guide communications industry participant operations and network investments.

Best Practice development is not unique to the communications industry. However, the specific topic areas covered in the NRIC Best Practices are. For example, communications industry Best Practices would be the "best in class" methods and procedures for carrying out operational functions like network engineering, service provisioning, network monitoring, and network maintenance. Best Practices are agreed upon through a consensus process and are not product-specific. They address classes of issues with practical solutions that are already in use by at least some members of the industry before they are considered by NRIC.

Over the years, the membership of NRIC has expanded to include CEO-level representatives of wireless, Internet Service Provider (ISP), Cable television (CATV) and satellite firms. As NRIC's representation has grown, the body of Best Practices has kept pace by addressing important reliability issues connected with these emerging communications platforms.

In the months after the September 11 attacks, NRIC VI was asked to take a close look at communications security. Focus Groups were formed to address business continuity, physical security, public safety communications, and cybersecurity. Thousands of staff-hours were contributed by subject-matter experts, who produced hundreds of new Best Practices, all of which are available at the NRIC web site – www.nric.org.

To conduct its work in the area of security NRIC assessed vulnerabilities in Internet networks and public telecommunications networks and determined how best to address those

vulnerabilities to prevent disruptions that would otherwise result from terrorist activities, natural disasters, or similar types of occurrences. Likewise, NRIC reported on existing disaster recovery mechanisms, techniques, and practices and developed additional Best Practices to more effectively restore Internet and telecommunications network disruptions arising from attacks and natural disasters. The work on cybersecurity has led to over 200 Best Practices to help service providers engineer, operate and maintain secure networks.

NRIC Cybersecurity Best Practices

The NRIC cybersecurity Best Practices can be categorized into several areas, including: (1) updating software; (2) secure equipment management; (3) intrusion prevention and detection; and (4) intrusion analysis and response.

Updating Software. New vulnerabilities regularly arise after network operators have placed new software in operation in their networks, so keeping system software up to date is vital to continued security of the network. For example, NRIC has a Best Practice entitled "Expedited Security Patching" to address this issue. This Best Practice specifies that service providers should have special processes and tools in place to quickly patch critical infrastructure systems when important security patches are made available.

Secure Equipment Management. Communications networks often manage network equipment remotely and automatically. These capabilities can provide significant operational benefits; however, this remote management capability can also expose networks to significant risks of unauthorized access. Many NRIC Best Practices cover remotely managed equipment and ensure, as fully as possible given current technologies, against damage or unauthorized access to network equipment.

Intrusion Prevention and Detection. Despite the best equipment management and patching practices, communications networks, by their very nature, can be susceptible to intrusion. Therefore, a necessary component of any security regime will be procedures to ensure timely and appropriate intrusion detection and response. These procedures should be calibrated to most quickly detect and respond to those network intrusions that, by virtue of their location, pose the greatest threat to the continued reliable and secure operation of the affected network. Leaving unused network services running can enable hackers to plant code for the initial phase of an attempt to incapacitate a network target by inundating it with traffic, also know as a "Distributed Denial of Service" attack. NRIC includes a Best Practices that gives service providers detailed advice on how to erect defenses against intruders and how to use systems that have been compromised.

Intrusion Analysis and Response. Physical damage or disruption of network components, whether the product of natural or man-made events, poses another significant threat to our communications networks. Accordingly, proper network-security practices dictate that network operators be prepared to quickly respond in the event that network components sustain physical damage or experience degraded operating efficiency. This would include having appropriate redundancies built into the network and having adequate repair and replacement plans for network components likely to sustain physical damage.

Outreach

While many of the largest telecommunications industry participants are members of NRIC, there are many others that have not been intimately involved in the process. The Commission has turned its attention to outreach and education to expand the range of awareness and encourage implementation of NRIC Best Practices, including those aimed at improving

cybersecurity. Venues for these educational seminars include state and national telecommunications associations, with a primary emphasis on reaching small independent service providers.

Hurricane Katrina

The massive damage and loss of life caused by last year's hurricane season is well known. As I am sure you are also aware, most of the communications industry sustained tremendous damage to their facilities in the affected area, and the damage had a significant impact. The damage to the communications infrastructure hampered the rescue operations of emergency responders. Relief efforts and survivors struggled with the effects of the hurricane. Survivors lacked information about relief efforts. People displaced from their homes did not have the means to contact their loved ones to let them know they were safe. And of course, survivors remaining in the affected area lacked a reliable means of contacting the authorities and getting help in life-threatening situations.

In the months after Hurricane Katrina, the Commission established the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks (Katrina Panel). The Panel was charged with (1) reviewing the impact of Hurricane Katrina on telecommunications and media infrastructures; (2) reviewing the effectiveness of the recovery effort; and (3) recommending to the Commission ways to improve disaster preparedness, network reliability, and communication among first responders. The Katrina Panel produced a report and recommendations in June of this year. Shortly thereafter, the Commission released a Notice of Proposed Rulemaking (NPRM) seeking comment on the Katrina Panel's report and recommendations.

A number of the recommendations will likely lead to more reliable Internet services. For example, the Katrina Panel recommended that the Commission work with and encourage each industry sector, including IT, to develop and publicize sector-specific readiness checklists. These checklists would be based on relevant best practices developed by the NRIC and MSRC, and would include business continuity plans, exercises, development of communications plans and routine archival of critical system backups and providing for their storage in "secure off-site" facilities. The Panel suggested that the Commission coordinate with other federal and state agencies to identify a single repository/point of contact for communications outage information in the wake of an emergency. In this regard, the Panel recommended that the FCC serve as the single point of contact and that it work with affected industry members and their trade associations to establish consolidated data sets and geographic areas for data collection. The Panel also suggested that the Commission work with Congress and other appropriate federal departments and agencies to improve the credentialing process and to provide emergency responder status under the Stafford Act for critical infrastructure providers. The Report also encouraged state and local jurisdictions to retain and maintain a cache of equipment components, including IP gateways that would be needed to immediately restore existing public safety communications within hours of a disaster. The Commission is currently reviewing the more than 100 comments and reply comments filed in response to this NPRM.

Conclusion

Internet-based telecommunications systems are becoming increasingly important to the Nation. Legacy telephone service is now supplemented by various forms of Internet telephone service. Internet-based applications have entered the mainstream and broadband access connections continue to make their way into our homes and businesses. With this change comes

increased opportunity, as well as increased risk. The opportunities stem from the Internet's ability to transport and deliver multimedia services over an integrated broadband network. At the same time, high performance computing platforms that were once largely isolated from the network are now interconnected and open to compromise if unprotected. The Commission, through the policies and actions described today, is working to protect the integrity and reliability of the critical communications infrastructure.

I would be happy to respond to your questions.