Statement of Senator Daniel K. Akaka
Securing Cyberspace: Efforts to Protect National Information Infrastructures Continue to Face Challenges"
Subcommittee on Federal Financial Management, Government Information, and International Security
July 19, 2005

Thank you, Senator Coburn for holding this hearing on the important issue of securing cyberspace.

Computers and computer networks reside at the heart of the systems upon which the American people rely on a daily basis. As our witnesses know, many of these systems are far too vulnerable to cyberattack, which would inhibit their function, corrupt important data, and expose private information.

The Internet is the backbone of the U.S. economy and our nation's critical infrastructures. It is the electronic roadway of commerce, industry, and defense. Databases stored on computer networks, in particular, have been an attractive target for criminal hackers, who have breached the networks of several well-known companies and have stolen the personal data of millions of Americans. A successful attack on the computer systems that support our critical infrastructures would threaten our national security, public health, and way of life.

The former head of the National Infrastructure Protection Center, Ron Dick, once said, "The thing that keeps me awake at night is the thought of a physical attack on the U.S. infrastructure combined with a cyberattack which disrupts the ability of the first responders to access 911 systems." This is not an exaggerated fear, as our own military realizes the power of cyber warfare in destroying an enemy's command and control.

The Department of Homeland Security (DHS) is responsible for protecting the key resources and critical infrastructures in the U.S. In carrying out this role, DHS has a number of responsibilities established by law and presidential directive. We are here today to discuss how DHS is fulfilling those responsibilities and the specific challenges that the Department faces as it moves forward.

One area that is of particular concern to me is the failure by DHS to complete a comprehensive cyber threat and vulnerability assessment. This threat assessment should be the foundation for the Department's risk-based approach to mission and priorities. A comprehensive threat assessment is needed in order to be certain that we are adequately protected and to ensure that precious federal dollars are well-spent.

I thank the witnesses for being with us today to share their insight, and I thank you again, Mr. Chairman, for holding this hearing.