The House Committee on
HOMELAND SECURITY
Peter T. King (R-NY), Chairman
FOR IMMEDIATE RELEASE
www.homeland.house.gov

Opening Statement of Chairman Dan Lungren

Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

"The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure"

April 15, 2011

Welcome to the second in our series of cybersecurity hearings. Today's hearing will focus on "the Department of Homeland Security's Cybersecurity Mission.

Homeland Security Presidential Directive 7, issued on December 17, 2003 outlines our national policy for Federal departments and agencies to partner with the private sector to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. The Secretary of Homeland Security was given the responsibility for "coordinating the overall national effort to enhance the protection of the critical infrastructure," whether owned and operated by the public or private sector. With the private sector owning more than 80% of the Nation's critical infrastructure, the DHS-Private Sector relationship is crucial.

As stated in our previous Subcommittee hearing on March 16th, information networks and computer systems face a combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat and vulnerability awareness. A successful attack on our power grid or our communications networks could not only cripple our economy but threaten our national security.

Under current law the vast majority of critical infrastructure fall outside the Department's direct cybersecurity regulatory authority. Under the Homeland Security Act of 2002, the Department was authorized to provide, upon request, analysis and warnings related to threats and crises management support to private sector owners and operators of critical information systems. They can also provide technical assistance to the private sector with respect to emergency recovery plans when responding to major failures of critical information systems. The Department does not have the ability to require the private sector use of any particular cybersecurity processes or tools. In this environment of ever changing technology and innovation, I believe this is sound policy.

It is important to note that just because the Department **can not** directly regulate the cybersecurity requirements of various sectors that the private sector is completely unregulated.

The electric power sector has had mandatory cybersecurity standards in place since 2008 and Sarbanes Oxley Act requires all publically traded companies certify that they have proper internal controls in place on their financial accounting systems. This requirement, in essence, equates to requiring proper cybersecurity in their IT/Finance systems.

Without direct regulatory authority, the Department exercises much of its responsibility for securing private critical infrastructure as a coordinating agent. The Department has established a number of cybersecurity functions and services to help in its role as coordinator. The National Cybersecurity and Communications Integration Center (NCCIC) enables the Department to bring together its federal partners as well as members of the private sector to integrate information and provide the focus of cybersecurity operations for the entire Federal government. I was privileged to be invited to the ribbon-cutting ceremony for this cybersecurity and communications integration center which we all hope will become the model for a successful public-private cybersecurity partnership.

The public-private partnership remains a key part of the nation's efforts to secure and protect its critical cyber-reliant infrastructure. While criticized by some, it is still evolving since its inception a decade ago. Because of the leadership of NPPD Under Secretary Rand Beers and Deputy Secretary Phillip Reitinger, the Department has strategically positioned cybersecurity resources and assets in an effort to develop a more trusted and mutually beneficial public-private partnership that is needed to defend cyberspace. Without ownership, partnership is the next best thing for promoting cybersecurity and protecting our critical infrastructure. If properly developed and implemented, the public-private partnership cybersecurity model can be leveraged to improve the culture of security and the willingness of the private sector to make the necessary investments to secure their critical infrastructure.

With all this cyber expertise, is the Department making a real difference in defending critical infrastructure? Are they protecting government and private sector cyber space and responding effectively to cyber attacks? Are they assisting the private sector in detecting, defending and recovering from cyber attack? Is the Department making available to its partners the critical threat information they need to protect their networks?

Today we will hear from the Homeland Security Department and a number of key economic sectors, whose critical infrastructure is vital to maintaining our robust economy, on how this public-private partnership is progressing.

I now recognize the Ranking Member Ms Clarke for her opening statement.