Opening Statement of Chairman Dan Lungren

At the Markup

Of

H.R. 3674

"Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011"

Before the

Subcommittee on Infrastructure Protection, Cybersecurity and Security Technologies

February 1, 2012

311 Cannon

I want to welcome everyone today to our Subcommittee's markup of H.R. 3674 "Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011" or PrECISE Act. We have been talking about the cyber threat for a very long time. In the first session of this Congress alone, we have had 5 cybersecurity hearings and countless briefings. These hearings have demonstrated that the cyber threat is real and it's growing. The nation's top government, intelligence and military leaders often mention the cyber threat as the issue that worries them the most. **Why?** Because a successful cyber attack on our power grid or our communications networks could cripple our economy and threaten our national security.

In addition to national security concerns, cyber attacks are robbing us of our intellectual property. This costs U.S. jobs and jeopardizes our economic future. As Members of the Cybersecurity Subcommittee of the Homeland Security Committee, we have a responsibility to protect American intellectual property and ingenuity as well as

the critical infrastructure which makes our economy so productive.

My legislation accomplishes this by authorizing the Secretary of Homeland Security to protect our Federal networks, systems and critical infrastructure from cyber attack. Under the bill, the Secretary will be required to coordinate cybersecurity activities across the Federal Government, publish a cybersecurity strategy and provide appropriate reports to Congress.

After hearing from so many organizations that our current information sharing arrangements are not effective, my bill addresses that need by creating the National Information Sharing Organization or NISO. The NISO will have three missions: 1) to facilitate the exchange of vital cyber threat information, best practices and technical assistance among its private sector and Government members; 2) to create a common operating picture of the network enabled by its most sophisticated members, ISPs and the Government; and 3) to facilitate cooperative research and development projects driven by the NISO membership.

In addition, my legislation requires the Secretary to work with the owner and operators of critical infrastructure and

their sector specific agencies to identify sector specific cybersecurity risks. The Secretary shall review and collect existing cybersecurity performance standards and evaluate them against identified sector specific risks. The Secretary would then inform critical infrastructure owners and operators of those risks and the mitigating cyber standards.

Only agencies with regulatory authority over **"covered critical infrastructure"** would be required to incorporate the most effective and cost efficient cyber standards into their existing regulatory regimes. DHS will determine who qualifies as **covered critical infrastructure** defined as infrastructure that if destroyed or disabled would result in a significant number of deaths, cause mass evacuations, major disruptions of the economy or significant disruption to national security.

This section of my bill has generated the most concern among our private sector partners. However, I believe it is the least intrusive of the cybersecurity proposals currently under consideration. The President's plan calls for establishing an auditing regime to ensure compliance with their cyber standards. The Senate bill would have DHS regulate cybersecurity across the various critical

infrastructure sectors adding to the list of government regulators and creating potentially conflicting regulations.

My bill calls on industry regulators to adopt existing cyber standards necessary to mitigate agreed upon cybersecurity risks. This concept does not address every risk only those critical to our country and it does it in the least disruptive manner. In my view, the alternatives, including preserving the status quo of voluntary action, are no longer acceptable.

Government should enable and facilitate the private sector in this effort by providing threat information, standards and best practices. In this way, we ensure that owners and operators are in the strongest position to protect their critical infrastructure. I hope you agree with this approach and I ask for your support of H.R. 3674.

I now recognize the gentle lady from New York, Ms Clarke, for her opening statement.