Committee on
HOMELAND SECURITY
Chairman Peter T. King

Opening Statement

April 26, 2012

Media Contact: Shane Wolfe

(202) 226-8417

Statement of Chairman Lungren

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Joint Hearing

"Iranian Cyber Threat to the U.S. Homeland"

April 26, 2012

Remarks as Prepared

Communicating through cyberspace is now an integral part of the international marketplace and the global economy. Businesses of all sizes increasingly depend upon it for their daily operations as well as for market growth. These innovative cyber technologies help U.S. businesses achieve great efficiencies and run their vital infrastructures. However, along with all the benefits, cyberspace is replete with nefarious actors – including organized criminals, industrial spies and foreign governments taking inappropriate advantage of a cyber environment open to all users.

We have been warning about cyber threats in this Committee for a long time. The nation's top government, intelligence and military leaders often cite the cyber threat as the issue that worries them the most. The reason is that a successful cyber attack on our power grid, transportation systems or communication networks could cripple our economy and threaten our national security. Any doubt about the physical damage that can be caused

by a cyber attack should have been eliminated by the stuxnet virus. Stuxnet is the best example of the cyber and physical worlds intersecting. Like Aurora, Stuxnet demonstrates that vital critical infrastructure can be physically disabled or destroyed by a capable and motivated enemy.

In addition to these national security concerns, cyber thefts are also robbing us of our intellectual property, costing U.S. jobs and jeopardizing our economic future. Cyber threats are real and growing in number and sophistication.

In assessing the Iranian Threat to the U.S. Homeland, we need to examine their motivation, opportunity and capability. As the victim of two recent cyber attacks (nuclear and oil infrastructure) and multiple U.S. embargoes, Iran clearly has motivation to strike us.

Their opportunity arises as U.S. critical infrastructure companies have been slow to harden their assets against cyber attacks. Unfortunately, cyber attacks can be launched from anyplace in the world because cyberspace doesn't recognize international borders.

The important question when assessing Iran as a cyber threat is their cyber capability. An American security-contracting firm issued a report in 2008 rating Iran's cyber capability among the top five globally. A December 2011 report indicated that Tehran was investing $1 billion in new cyber warfare technology. According to DNI Director Clapper, "Iran's intelligence operations against the U.S., including cyber capabilities, have dramatically increased in recent years in depth and complexity".

Since Iran appears to have the necessary cyber capability, we can only hope that they will fear attribution and the overwhelming U.S. response that would surely follow such an Iranian cyber attack against our nation.

I look forward to the testimony of our distinguished panel this morning on the nature of the cyber threat from this rogue Iranian regime.

###