RANKING MEMBER YVETTE CLARKE (D-NY)
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION AND SECURITY TECHNOLOGIES
COMMITTEE ON HOMELAND SECURITY

The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure

Opening Statement

I know Mr. Lungren takes this responsibility as seriously as I do, and I look forward to partnering with him again over the next two years to ensure the safety and security of the American people, American businesses, American infrastructure, and the American way of life.

Today's hearing will focus on our critical infrastructure sectors, their cybersecurity posture, and the DHS role in helping them to be as secure and simultaneously as open and efficient as possible.

We rely on information technology in every aspect of our lives – from our electric grid, financial and communication systems, and government functions, to name just the few that our witnesses here today represent.

Inter-connected computers and networks have led to amazing developments in our society. Increased productivity, knowledge, services, and revenues are all benefits generated by our modern networked world.

But in our rush to network everything, few stopped to consider the security ramifications of this new world we were creating, and so we find ourselves in an very vulnerable situation today.

As I stated at our last hearing: too many vulnerabilities exist on too many critical networks which are exposed to too many skilled attackers who can steal from or damage too many of our systems.

Unfortunately, to this day, too few people are even aware of these dangers, and fewer still are doing anything about it.

This Committee will continue to discuss and examine these issues in an attempt to raise awareness of the problems we face and, we hope, to help identify and implement practical and effective solutions.

There is a very real and significant threat to our national and economic security than we now face in cyberspace, and we must do something equally real and significant to meet this challenge.

As I noted at our hearing last month, we are expecting, and this Committee is eager to see, a National Cybersecurity Strategy from the White House to be released very soon.

I also stated at our last hearing that the Department is finalizing its National Cyber Incident Response Plan and will also include a Cybersecurity Strategy as called for in the 2010 Quadrennial Homeland Security Review.

Mr. McGurk, I hope to hear some good news from you on these items, because we can't keep waiting for these things.

The Congress is interested in moving legislation to afford DHS authority it needs to protect the dot-gov domain and critical infrastructures in the private sector.

Hopefully we are done playing these government shutdown games here in Congress and we will get on to the business that our constituents elected us to do.

This cybersecurity issue is complicated and no one entity or approach will work.

I firmly believe that the U.S. government and the private sector must be full partners in this effort, and both must accept their share of the burden, responsibility, and cost for our combined security.

The intention behind this hearing is to focus on the protection of the critical infrastructures that sustain our lives and our economy.

Those infrastructures are under constant attack.

Cybercrime costs this country alone billions of dollars a year.

We know that our government networks are attacked tens of thousands of times per day, and private sector networks are attacked even more often.

We know that our critical infrastructures are all already compromised and penetrated.

We need to absorb this information, get up to speed quickly, and move forward to address this issue.

We have to start protecting ourselves before an attack big enough to cause irreparable damage is carried out.

To the witnesses appearing before us today, I thank you for being here, and I welcome your thoughts on the issues before us including what you think an effective national cybersecurity policy should look like, and especially the critical details needed to make this public-private partnership work.

Chairman Lungren and I intend for this Subcommittee – as well as the full Committee – to play a leading role in shaping our national cyber posture in the years to come.