

**OPENING STATEMENT OF RANKING MEMBER
YVETTE CLARKE (D-NY) AS PREPARED
CYBERSECURITY, INFRASTRUCTURE PROTECTION AND SECURITY
TECHNOLOGIES SUBCOMMITTEE
COMMITTEE ON HOMELAND SECURITY**

***HEARING: Examining the Cyber Threat to Critical Infrastructure and
the American Economy***

I would like to thank you Chairman Lungren for holding this hearing on cybersecurity and for your intention to move expeditiously on what I know we both recognize as a critical issue.

While there are a number of new faces up here on the dais, I believe that this Subcommittee will continue to place significant focus on the issue of cybersecurity just as we did during 110th Congress.

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 likely be the first of several cybersecurity hearings that the Subcommittee will hold this month, and it is easy to understand why this issue dominates our agenda.

We rely on information technology in every aspect of our lives – from our electric grid, banking systems, military, and government functions, to our email and web browsers.

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 extremely dangerous situation today.

Too many vulnerabilities exist on too many critical networks which are exposed to too many skilled attackers who can inflict too many intrusions into 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 sound the alarm bells, raise awareness of the problems we face, and move forward with practical and effective solutions.

This hearing comes at a critical moment in our nation's approach to the cyber threat.

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.

We are expecting, and this Committee is eager to see, a National Cybersecurity Strategy from the White House to be released very soon.

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.

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

The previous two decades have seen countless reports from America's thought leaders in cybersecurity, containing hundreds of recommendations about how to improve America's posture in cyberspace.

What has been lacking is the courage and leadership to actually implement these recommendations.

To ensure our national and economic security, now is the time we must act.

The U.S. government must chart a new course to secure cyberspace.

The private sector must also be a full partner and accept its share of the responsibility for our combined security.

Maintaining the status quo will not be enough to keep America secure.

Now is the time to stop planning and start acting.

The Chairman's intention with this hearing is to give this subcommittee some background on the issues facing us.

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.

The enemy has already successfully attacked, and continues to do so.

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

We have already lost many small battles. 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.

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.