Ranking Member Yvette D. Clarke (D-NY)

Opening Statement, as prepared

Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

"Examining the Homeland Security Impact of the Administration's Cybersecurity Proposal"

June 24th, 2011

We live in a world where it seems that everything relies on computers and the Internet.

The effective functioning of our critical infrastructure – from airports, financial systems, to water systems, factories, the electric grid – is highly dependent on computer-based systems called "control systems" that are used to monitor and control sensitive processes and physical functions.

The danger of both unintentional and intentional cyber attack is real, and the potential consequences of an attack on control systems vary widely from the introduction of raw sewage into potable water systems to the catastrophic failure of critical electrical generators due to the change of a single line of code in a critical system.

We've come to recognize that public/private partnerships are a key component of securing our Nation's computer-reliant critical infrastructure. Private sector involvement is crucial, as it collectively owns the vast majority of the Nation's cyber infrastructure and is responsible for protecting its networks and systems from the growing threat of a cyber attack.

Enhancing the public/private partnerships by developing an improved value proposition and implementing better incentives, among other measures, will be essential to encouraging greater private sector involvement.

Control systems are not the only computers subject to attack. Every day, thousands of attacks are launched against Federal and private networks by hackers, terrorist groups, and nation states attempting to access classified and unclassified information, and the infiltration by foreign nationals of federal government networks is one of the most pressing issues confronting our national security.

Federal networks have been under attack for years; these attacks have resulted in the loss of massive amounts of critical information, though many of these attacks are classified.

We all know that cybersecurity is a critical national security issue, and this Committee has taken the lead. My Ranking Member, Mr. Thompson re-introduced his cybersecurity bill from last year, H.R. 174, in January of this year, and made sure it was referred to this Subcommittee. The need to improve America's cyber defense posture is clear, and the Homeland Security Committee has been arguing this point for a long time.

Now, the President has come forward with a comprehensive strategy, and some legislative proposals, about how it will prevent, detect, and respond to attacks on computer systems and infrastructure.
There have been many cyber-related bills in the last session of Congress, and Members of Congress wrote to the President and asked for his input on cybersecurity legislation. As part of the President's two-year Cyberspace Policy Review, The White House has put forth a detailed and determined cybersecurity legislative proposal.