Ranking Member Yvette D. Clarke (D-NY)

Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"Striking the Right Balance: Protecting Our Nation's Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties"

April 25, 2013 – 2 P.M.

Here on the Homeland Security Committee, we have understood the need to balance security and privacy for a long time. Protecting our Nation from 21st century threats requires vigorous, coordinated action from our government and state, local, private sector and international partners.

But if we go over board to identify and eliminate every conceivable threat at any cost, we risk trampling the very rights of the citizens we aim to protect. The need to find that proper balance has been a cornerstone of our Committee's work, on counterterrorism, on transportation security, and certainly on today's topic, cybersecurity.

Most of the government's efforts in cybersecurity do not directly touch upon privacy issues, and that is an important distinction that is not made often enough. Many programs, such as the Department of Homeland Security's EINSTEIN program, do not involve the collection or sharing of any kind of personally identifiable information at all.

And the vast majority of the information needed to thwart cyber attacks consists of technical data such as IP addresses and malicious code, which has little or nothing to do with someone's social security number or passwords. But where the private sector needs to share information with the government to stop cyber attacks, every precaution must be taken to ensure that the privacy of our citizens is ensured.

Last month we heard from the American Civil Liberties Union on the importance of protecting privacy in cyberspace, and I am pleased that we are joined today by three witnesses who can really speak to the nuts-and-bolts challenges of protecting private data, both from the governmental and business perspectives.

As we look towards crafting our own legislation to help protect critical infrastructure and improve our Nation's cybersecurity efforts, it is important to really nail down the specifics on protecting privacy.

In order to get our approach to cybersecurity and privacy right, we must examine it from all the angles:

- We must assess the current legal environment and identify challenges that companies must cope with in ensuring the privacy and security of their employees and customers' data;
- We must determine the types of information needed by the government to prevent attacks, and the intended uses for that information;
- And we must examine how commercial cybersecurity providers interact with their customers and the government to share threat information.

Thankfully, our witnesses today cover the breadth of these issues with their testimony. I am particularly pleased that we are joined by Harriet Pearson, who was one of the Fortune 1000's first Chief Privacy Officers, and has been a trailblazer for developing information policies and practices for protecting the private data of employees and consumers.

Every American values their privacy and civil liberties as well as their security in cyberspace, and I am confident that in building a lasting solution to our cyber insecurity, we can adopt measures that will satisfy privacy advocates, the business community, and our citizens.