REP. YVETTE D. CLARKE (D-NY)
Opening Statement

Hearing on Draft Legislative Proposal on Cybersecurity

Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

December 6, 2011

From my perspective, the Department must have sufficient authority to make sure that government and privately owned critical infrastructure install and monitor ample protection for their cyber systems, both agency-wide in the federal government, and for identified critical infrastructure that supports the economic, social, and security needs of our nation.

Effective implementation of that authority will enable DHS to lead by example – a prerequisite for building credibility and trust with privately owned critical infrastructure.

In H.R. 174, the Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, introduced by Mr. Thompson in January of this year, and which I cosponsored, the Department is specifically given major cybersecurity responsibilities, and includes a plan to oversee cybersecurity efforts for identified critical infrastructure, much like we already do in the CFATS program, which I think is a prudent, risk-based approach.

The draft legislation we have before us includes an emphasis on voluntary incentives for private companies, with some narrowly targeted regulation for critical infrastructure industries that are already highly regulated. I think we're all looking for a way to not have regulation that duplicates what is already being done. Government can ask the critical infrastructure systems to improve security only if government is a model leading by example.

Mr. Chairman, I'm glad to see the language of the discussion draft does provide some provisions that are broadly similar to provisions in H.R. 174, and the White House Cyber Proposal; for example, 1) by increasing the responsibilities of the Department for cybersecurity in the federal agencies and critical infrastructure; 2) authorizing US-CERT; 3) addressing supply chain vulnerabilities; 4) increasing cyber R&D; and 5) providing enhance personnel authorities to improve the cybersecurity workforce.

My concern is two-fold. How can we realistically increase out cybersecurity efforts if the House appropriations drastically reduced level of funding is implemented?

And secondly, the discussion draft relies on purely voluntary actions and establishes a nonprofit, quasi-governmental entity, the National Information Sharing Organization (NISO), with private- and public-sector members for the purposes of facilitating information exchange, performing collaborative cybersecurity R&D, and encouraging nonfederal use of voluntary cybersecurity standards.

I think it's important that we look closely at the details of this quasi-governmental entity, to explore the real-life implications of such a body and its actions, and how it would affect the Department's ability to enhance cybersecurity for our government agencies, our crucial critical infrastructure, and ultimately for our citizens.