Ranking Member Yvette D. Clarke (D-NY) Opening Statement

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

"Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities"

May 16, 2013 at 9:00 AM

After a significant expansion of the Department of Homeland Security's cybersecurity mission and programs, beginning in Fiscal Year 2012, I am glad that we are finally holding a hearing to look at these programs in depth and to assess the progress of the Department in carrying out that mission.

This is the subcommittee's third hearing on cybersecurity this Congress - first, we held a hearing on the threats in cyberspace to our critical infrastructure from state and non-state actors. Next, we learned about how DHS protects the privacy of our citizens in cyberspace.

And with that background in place, today we will hear from the witnesses about whether the Department has the people, programs, and resources in place to successfully address the significant cyber threats to our critical infrastructure while protecting privacy. It is high time that our subcommittee takes a closer look at these programs, some of which did not even exist just a few years ago.

The continuous diagnostics and EINSTEIN programs, in particular, have undergone rapid expansion, and I am pleased that the Department is fulfilling its role as the protector of the dot-gov domain, with the resources to match. But though these Federal network security programs get the majority of the funding and attention, I believe the Department's responsibilities for protecting critical infrastructure, most of which is found in the private sector, is equally important.

For this reason, I am particularly pleased that we are joined by Deputy Inspector General Charles Edwards, who can discuss recent work done by the OIG to assess the progress that ICS-CERT has made to brand itself as the Cyber 9-1-1 for critical infrastructure before, during, and after cyber incidents.

ICS-CERT, recently incorporated as an operational arm of the NCCIC, has done great work in mitigating cyber risks to critical infrastructure, and I look forward to learning more about this mission and the challenges that still remain to share information with the private sector quickly and efficiently.

Finally, I want to register my concerns over the continuing drain of senior cybersecurity leadership at the Department, a trend that has gotten particularly bad in the last six months, with the departures of the Assistant Secretary and the Deputy Under Secretary.

We have been hearing about the difficulties DHS faces in attracting and retaining skilled junior and mid-level cyber employees for a long time, but what does it say about the Department's cyber organization when it cannot retain its senior leaders, either? Rumors are circulating about future replacements for these losses, and I am sure DHS would like to make a splash with these appointments, getting leaders who command respect in the information security and critical infrastructure worlds. But most of all, DHS needs to find leaders who believe in the mission and will stay on board as a steady hand on the wheel during this period of immense expansion and evolution of our cybersecurity efforts.

As part of this process, I believe DHS needs to do some soul-searching and identify why their senior officials have been leaving, and if changes need to be made to ensure future leaders will be more empowered to do their job, I expect that the Department will do so. I hope to work with the Department in this endeavor to guarantee that the vital cybersecurity mission gets the leadership it needs.