CONGRESSWOMAN YVETTE D. CLARKE

REPRESENTING NEW YORK'S 11th CONGRESSIONAL DISTRICT

March 10, 2009

Contact for Homeland Security Press:
Dena Graziano 202.226.4503 office
202.286.4133 cell

STATEMENT OF CHAIRWOMAN YVETTE D. CLARKE
3-10-09 CYBERSECURITY HEARING

Good afternoon, and thank you to all of our witnesses for appearing before us today. I am pleased to chair today's hearing, my first as the Chair of the Emerging Threats, Cybersecurity, Science and Technology Subcommittee.

While there may be a number of new faces up here on the dais, I can assure everyone that this Subcommittee will continue to address many of the same issues from the 110th Congress. Over the next two years, we will continue our oversight over nuclear detection programs, radiological threats, public health threats, cybersecurity, and the Science and Technology directorate.

I also look forward to working in the same bipartisan spirit that the previous Chairman and Ranking Member carried on their work. I know Mr. Lungren takes this responsibility as seriously as I do, and I look forward to partnering with him 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 be the first of three 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, web browsers, and I-Tunes. 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 damages to 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 hold those in charge accountable for their inaction.

This hearing comes at a critical moment in our nation's approach to the cyber threat. There is no more significant threat to our national and economic security than that which we face in cyberspace. And we – the United States – must do something equally significant to meet this challenge.

We are approximately halfway through the National Security Council's 60 day interagency review of the Federal cybersecurity mission, which began on February 16. The review is being conducted by Melissa Hathaway, Senior Director of the NSC, on orders from President Obama and the National Security Advisor. The goal for the review is "to develop a strategic framework to ensure that U.S. Government cybersecurity initiatives are appropriately integrated, resourced and coordinated with Congress and the private sector."

I commend the President for his vision in making cybersecurity a priority for his Administration, and for requesting this review. Given this Committee's leadership role in cybersecurity policy development, we look forward to working with Ms. Hathaway and her team. Thankfully, their review does not have to start from scratch. I encourage the review team to rely upon the extensive hearing record of this Committee in the 110th Congress, and from the work that our witnesses have already undertaken in this area. The CSIS Commission report and the many GAO reports which Mr. Powner's team have produced over the years contain dozens of outstanding recommendations that, if actually implemented, will improve our national cybersecurity posture.

That message bears repeating. 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.

<u>Now is the time to act.</u> 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. Maintaining the status quo will not be enough to keep America secure. Now is the time for the government to stop planning and start acting.

There are three key issues that I believe this review must address. First, this review must call for a national strategy for cyberspace. The previous Administration drafted a high-level "National Strategy" in 2002 that presented problems and possible solutions to some of the same cybersecurity issues we face today. Unfortunately, that strategy stopped short of mandating security changes. Without teeth, the strategy was never implemented. We need a strategy that uses all of the tools of U.S. power in a coordinated fashion – but more importantly, we need to hold our agencies accountable in implementing that strategy.

This leads to my second requirement: leadership. A lack of high level leadership on cybersecurity has cost our country dearly over the last several years. The review must clearly delineate roles and responsibilities of each agency involved in the governance of cybersecurity at the Federal level, including DHS, NSA, and DOD, but, most importantly, it must describe how the White House will coordinate the policy and budgets for each of these different responsibilities. The CSIS Commission recommended – and I fully support – an Assistant to the President for Cyberspace Security in the Executive Office of the President, along with a support staff, to coordinate this effort.

Third, the review must address the many policy and legal shortfalls that exist in protecting our critical infrastructure from cyber attack. Unfortunately, critical infrastructure systems remain the area of greatest vulnerability. While the previous Administration relied on a voluntary protection system throughout many of the 18 critical infrastructure sectors, I believe this Administration should seek to use a combination of regulations and incentives to ensure that our electricity grid (including the Smart Grid), water facilities, financial systems, and other key infrastructures are properly secured. The framework of this approach should be addressed in the review.

To the witnesses appearing before us today, I thank you for being here, and I welcome your thoughts on the issues I've just discussed, as well as your opinions on what an effective national cybersecurity review should look like. I intend for this Subcommittee – as well as the full Committee – to continue to play a role in shaping our national cyber posture in the years to come.