Protecting Information in the Digital Age: Federal Cybersecurity Research and Development Efforts

Opening Statement of Ranking Member Wu

March 25, 2011

Thank you, Chairman Quayle, for calling this hearing. And thank you to our witnesses for being here today.

More and more of our personal information is making its way online, and our Nation's entire infrastructure—from traffic systems and the electricity grid to manufacturing—is becoming increasingly dependent on its connection to the internet. I can think of no topic more important for this Committee to address than cybersecurity. You just need to read the headlines to know that cybercrimes are becoming more frequent— Sony's PlayStation network has been repeatedly targeted by hackers with the personal information of more than 100 million users being exposed, a server at NASA was recently targeted revealing satellite data, and social media sites like Facebook are consistently targeted by phishing scams and other cyber attacks.

I'm pleased that the Administration has provided Congress with a legislative proposal to consider. The proposal focuses primarily on the role and authority of the Department of Homeland Security in the securing non-defense systems. I look forward to working with the Chairman and the other members of this Committee to ensure that NIST's expertise in information security, especially in the development of technical standards and as a convener and consensus builder of private sector interests, is maintained. I'm also interested in ensuring that cybersecurity research and development and a clear strategy to building a highly-skilled federal cyberworkforce is incorporated into any comprehensive bill that moves through the House.

OMB reports that, in 2010, Federal agencies spent $12 billion on cybersecurity to protect the $80 billion dollar federal information technology infrastructure. Additionally, the Federal government funds about $400 million in cybersecurity research each year.

Despite these considerable funding levels and many hours spent by federal employees on this issue, the assessment remains the same: our cybersecurity is poor. We need to use our existing resources more efficiently and with specific achievable goals in mind.

Previously, federal efforts have been output oriented—focused on things like the number of programs, funds spent, or the number of interagency working groups—rather than outcome driven. I am pleased that the current Administration is focusing its efforts on achieving outcomes such as fewer breaches of federal systems, fewer cases of identity theft, and ensuring the security of smart grid and health IT systems.

While the Administration's Cyberspace Policy Review was just a reemphasis of recommendations made in previous reports — improving information sharing, bolstering interagency and private sector coordination, modernizing the research agenda, and enhancing public cybersecurity awareness and education — it was successful in outlining a concrete vision and set of objectives that have been steadily addressed by the Administration over the last two years. For example, the creation of a National

Initiative for Cybersecurity Education to make consumers aware of online risks and training to ensure a skilled cybersecurity workforce; the development of an identity management framework, known as the National Strategy for Trusted Identities in Cyberspace, to lessen online fraud and strengthen privacy; and the recent release of an *International Strategy for Cyberspace* that calls for the development of international standards that prevent barriers to trade and commerce and an open environment that fosters free expression and innovation around the world.

By addressing these recommendations, we are laying the building blocks for a new, outcomes-based approach to federal cybersecurity. The agencies appearing before the Committee today have a significant role to play in creating that foundation.

During today's hearing, I hope to learn how each agency has progressed toward meeting the goals and objectives outlined in the Administration's review, their future plans, and the impact of the Administration's legislative proposal on their current roles and authorities. This information will help guide the Committee's ongoing efforts to protect our Nation from cyber attacks.

I'd like to again thank the witnesses for being here today and I look forward to your testimony. Thank you, Mr. Chairman. I yield back the balance of my time.