OPENING STATEMENT

Ranking Member Dan Lipinski (D-IL)
Subcommittee on Research & Technology
Committee on Science, Space, and Technology

"Can Technology Protect Americans from International Cybercriminals?"

March 6, 2014

Thank you Mr. Chairman. And thank you to our witnesses for being here today after some rescheduling earlier in the week.

I've spoken in this committee many times about the threats posed by cybercrime, and each time there have been recent and potentially more serious attacks to illustrate the point. This time, data breaches at Target and Neiman Marcus collectively resulted in over 100 million records being stolen in the form of personal and credit card information. In total, payment card fraud was responsible for over 11 billion dollars in losses in 2012, with around half of that amount coming from the US. And this figure doesn't account for many other losses associated with identity theft.

Simply put, cybercrime threatens businesses of all sizes and every single American. As such, reducing our risk and improving the security of cyberspace will take the collective effort of both the Federal Government and the private sector, as well as scientists, engineers, and the general public.

Research efforts by the Federal Government and standards developed in conjunction with the private sector will play a big part in addressing cybercrime. The NSF and NIST have lead roles in these respective tasks. I'm interested in hearing more from Dr. Romine about NIST's recent efforts in these areas including the cybersecurity framework for critical infrastructure released last month.

However, it's worth pointing out that it doesn't matter how good our technology is or how current our standards are if people don't use the technology correctly or adopt the standards. You can have the most up-to-date server in the world, but if someone doesn't change the default password or chooses an easily guessed password, no system will be safe. Consider that a Verizon report found that last year only 11% of companies surveyed were fully compliant with PCI standards. In many ways, people are the weakest link in this process, and understanding how people make decisions – and encouraging better decisions – through social science research must be a part of our efforts to mitigate risk.

To help address some of our nation's cyber threats, Congressman McCaul and I have introduced the Cybersecurity Enhancement Act during the last three congresses. The bill would improve cybersecurity by building strong public-private partnerships, improving the transfer of cybersecurity technologies to the marketplace, training a cybersecurity workforce for both the public and private sectors, and coordinating and prioritizing federal cybersecurity R&D efforts. We passed the bill in the House last year but are still awaiting action in the Senate. Hopefully

with increased focus on cybersecurity issues we can finally break through the logjam and get the Senate to act on a bipartisan bill that will address our most immediate research and workforce needs.

Once again, thank you Mr. Chairman for holding this hearing. I look forward to hearing from our witnesses. And with that, I yield back.