Committee on Science, Space, and Technology
Subcommittee on Research
Cyber R&D Challenges and Solutions
February 26, 2013

Opening Statement
By
Ranking Member Daniel Lipinski

I want to thank both Chairman Massie and Chairman Bucshon for holding this hearing to examine the serious cybersecurity challenges faced by our nation. In particular, I look forward to hearing feedback from our witnesses on H.R. 756, The Cybersecurity Enhancement Act, that I recently reintroduced along with Mr. McCaul.

I echo my colleagues' remarks about the nature and severity of the challenges we face in cybersecurity in both the public and private sectors. Four years ago when I began working on this legislation I said that I had no doubt that our use of the internet and other communication networks would continue to grow and evolve, and that threats from individual hackers, criminal syndicates, and even other governments would grow and evolve too.

Today it remains difficult to imagine just how much more we will simultaneously benefit from, and be made more vulnerable by, information technology. Hacking is no longer just the realm of computer whizzes. Today, anyone can "rent" a botnet or gain access to other sophisticated hacking tools with just a few key strokes and less than a hundred dollars.

Cybercrime threatens our national security, our critical infrastructure, 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.

With respect to that collective effort, I need to emphasize the importance of research into the social and behavioral aspects of cybersecurity. People are perhaps the most significant part of our IT infrastructure, but they are also the 'weakest link.' Many cyber attacks are successful because of human error – bad cyber hygiene – such as unwittingly opening a malicious email. Having the most sophisticated security systems available won't make any difference if users don't change factory-set default passwords or they set easy to crack passwords. Understanding

the human element and educating users to practice good cyber hygiene is necessary to combating threats and reducing risk.

Mr. McCaul and I are hopeful that our R&D bill will be part of a comprehensive, bipartisan cybersecurity bill. Previous efforts to move a larger bill have stalled over some significant policy disagreements, but I am hopeful that we will be able to resolve our differences and I look forward to working with both my colleagues and the Administration to ensure the development of a strong cybersecurity strategy this Congress.

However, I am also concerned that top line cuts to our federal R&D budgets will have a negative impact on any long-term cybersecurity strategy. So we must also take actions to mitigate the impact of those cuts.

Today, we will hear from witnesses who are actively engaged in efforts to improve the security of our digital infrastructure. I look forward to their valuable insight into the challenges we face in tackling this complex issue and the role of cybersecurity R&D and education in any comprehensive solution.