OPENING STATEMENT

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

Is the OPM Data Breach the Tip of the Iceberg
Joint Subcommittee Hearing

July 8, 2015

Thank you Chairwoman Comstock and Chairman Loudermilk for holding this hearing on the recent OPM data breach. I want to thank all the witnesses for being here this afternoon.

Unfortunately, major cyber-attacks are happening more frequently. Today, we are going to talk about the significant breaches at the Office of Personnel Management (OPM). Not to take away from the significance of the OPM breach, I think it is important to note that there have been an increasing number of cyber-attacks in both the private and public sector.

Several years ago I began working on cybersecurity legislation, the *Cybersecurity Enhancement Act*, with my colleague, Mr. McCaul. Our legislation dealt with cybersecurity standards, education, and workforce development. When we started, I said that I had no doubt that threats from individual hackers, criminal syndicates, and even other governments would grow and evolve along with our increased use of the internet. Unfortunately, I was right.

In February, Anthem, one of the nation's largest health insurance companies, announced that it suffered a cyber-breach that compromised the records of 80 million current and former customers. And just last year there were high profile breaches at JP Morgan Chase, eBay, Target, and many others affecting millions of people.

Although I was happy that my bill with Mr. McCaul was enacted at the end of last Congress, there is much, much more to be done in the area of cybersecurity. Cybercrime and cyber-espionage continues to threaten our national security, our critical infrastructure, businesses of all sizes, and every single American. This latest data breach at OPM is just another example of that. In the OPM breach, millions of federal employees' personal information has been compromised, leading to significant concerns about how the stolen information will be used. Additionally, since OPM conducts more than 90 percent of all security clearance background investigations, this breach is an example of how cyber-attacks threaten our national security. We must do better.

It will take a collective effort of both the public and private sector to improve cybersecurity, and I cannot emphasize enough the importance of research into the social and behavioral aspects in this area. Our IT infrastructure is built, operated and maintained by humans, from the average worker at her desktop to the chief information officer of a major company or agency. Most cyber-attacks are successful because of human error, such as unwittingly opening a malicious

email or allowing one's credentials to be compromised. Understanding the human element is necessary to combat threats and reduce risk.

To set government-wide guidelines for protecting federal information security systems, Congress passed the *Federal Information Security Modernization Act* or FISMA. FISMA, which was updated at the end of last Congress, requires federal agencies to develop, document, and implement an agency wide information security program.

Along with being responsible for their own information security system, the National Institute of Standards and Technology (NIST) is tasked with developing standards and guidelines for all civilian federal information systems. Since NIST plays a critical role in protecting our nation's information security systems, it is important that they be part of this conversation. I am happy that Dr. Romine is here today to tell us more about how NIST develops FISMA standards and how they work with other federal agencies.

FISMA also requires annual reviews of individual agencies' information security programs as well as reviews of information security policies and the implementation of FISMA requirements government-wide. I hope to hear from our witnesses about the steps necessary to ensure that OPM meets FISMA requirements, as well as how other agencies are doing in this space.

More information security systems—both in the public and private sector—will surely be subject to cyber-attacks in the future. And while it is impossible to completely protect a connected information security system, we must do all we can to protect the personal information of millions of Americans and conduct the oversight to ensure such steps are taken. This hearing is the beginning of a conversation on how we can do that and we must make sure that we follow through with action.

I look forward to our discussion this afternoon. Thank you and I yield back the balance of my time.