OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)
Committee on Science, Space, and Technology

"Can Technology Protect Americans from International Cybercriminals?"

March 6, 2014

Thank you, Mr. Chairman. This morning we are examining how technology can help protect Americans against cyber-attacks.

Unfortunately, we have seen a string of cyber-attacks recently. Last year, Target suffered a massive data breach resulting in the loss of millions of debit and credit card numbers. Neiman Marcus, a store based in my home state of Texas, experienced a data breach that involved over a million credit and debit cards last year as well. These breaches exposed the financial and personal information of millions of Americans.

Data breaches are devastating. They cause Americans to lose trust in private and public institutions and result in significant economic losses. Data breaches can also result in intellectual property losses, which can include a company's research and development, leading to millions and billions of dollars in lost profits. The Ponemon Institute estimates that the cost of data breaches due to fines, loss of intellectual property, customer trust and capital equal $136 per lost record. This translates into $68 billion in losses globally last year alone.

This morning we will hear about computer chip-based credit cards, known as the "chip-and-pin" cards. Although it seems like these "chip-and-pin" cards would help reduce counterfeiting of stolen credit cards, it is not clear that they would have prevented the recent attacks on Target and Neiman Marcus. To help prevent further similar cyber-attacks, we will need other technologies.

But new technologies alone will not prevent cyber-attacks. New technologies will need to be paired with training and education efforts. Email attachments carrying malware are the most common way attackers get into a computer. To stop that from happening, we need training and education about proper computer security for employees and individuals.

There are a number of federal efforts in this area including at the National Institute of Standards and Technology, which has played an important role in cybersecurity efforts for decades. NIST is the agency tasked with developing standards and guidelines for Federal information systems.

Additionally, NIST is the lead agency for the National Initiative for Cybersecurity Education; they developed the National Strategy for Trusted Identities in Cyberspace; they run a National Cybersecurity Center of Excellence; and they maintain a National Vulnerability Database.

We are fortunate to have Dr. Romine here this morning who can tell us more about these and additional cybersecurity efforts at NIST. Last month, NIST released a Framework for Improving Critical Infrastructure Cybersecurity, which provides a common language for understanding and managing cybersecurity risks. In our discussion of new technologies, we should be discussing how the federal government can incentivize the public sector to adopt cybersecurity best practices and standards that are included in the Framework.

To prevent cyber-attacks will take an all-hands-on-deck approach. I look forward to working with my colleagues on both sides of the aisle on how the federal government can help with the development and adoption of new cybersecurity technologies.

I would like to thank the witnesses for being here today. Thank you, Mr. Chairman. I yield back the balance of my time.