Opening Statement of the Honorable Tim Murphy
Subcommittee on Oversight and Investigations
Hearing on "Understanding the Cyber Threat and Implications for the 21st Century Economy"
March 3, 2015

(As Prepared for Delivery)

This is the first in a series of hearings by this Committee focused on cyberspace, the Internet and the challenges and opportunities that they present for the 21st century economy. These are big, important issues, so it is imperative that we establish a clear understanding of the issues we face.

So, today, we are going to do something a little different. We are not here to examine a specific cybersecurity incident, policy issue or legislative proposal. Today, we are going to take a step back and explore some fundamental questions. Why does the cyber threat exist? Is it something that can be solved? And what does this mean for the future?

In 1969, computers at four universities connected to the ARPANET, thus proving a computer networking concept that evolved into what we now know as the Internet. Since its inception, the Internet has been an open platform, designed to facilitate the transfer of data and information between remotely located computing resources. It does not discriminate against any network or device, nor the data they transmit. It is merely a conduit for information

This open architecture, end-to-end system design is what makes the Internet such a benefit to society. It provides endless possibilities for innovation. It gives any individual with an Internet connection an opportunity to share their opinion with the world. It has revolutionized the way we conduct business, interact socially, learn and consume information.

As a result, the Internet fostered widespread development and adoption of computing and communications technologies, collectively known as information technology. Today, we depend on these technologies for everything from social interaction to the operation of critical services like the electric grid. This integration of the Internet and information technologies into nearly every aspect of modern life has created the virtual world commonly known as *cyberspace*.

The Internet's strength, however, is also its weakness. It is by nature an open system with many interconnections, creating multiple opportunities for disruption. Likewise, information technologies are inherently complex systems, increasing the probability of ingrained vulnerabilities. As a result, the same technological and cultural factors that facilitate real-time global interaction, rapid innovation and freedom of expression empower malicious actors to thrive and create risk in cyberspace.

The challenge arises from the fact that cyberspace creates an asymmetric imbalance that strongly favors malicious actors. The nature of the Internet and complexity of information technology enables anyone – from an individual to a nation state – to target a victim halfway around the world at minimal cost and with little risk of being caught. Because the cost of failure is minimal, the threat evolves rapidly. In contrast, the costs of defense, as well as potential consequences, are significant.

Because this asymmetric threat is rooted in the fundamental structure of the Internet and information technology, there is no way to solve cybersecurity without undermining the benefits of the cyberspace. There is no silver bullet or technological solution. While we certainly can do more improve the security of cyberspace, these decisions require a thoughtful cost benefit analysis. How will a potential security measure affect the cost or convenience of a product? How will it affect the pace of innovation? What will it mean for privacy or civil liberties?

Cyberspace is no longer a place that we visit. It is a place where we live. Ten years ago, smartphones were a novelty – in fact, the iPhone didn't even exist. Today, mobile devices serve as a credit card, track

our health, unlock our homes and start our vehicles. A pacifier can monitor your infant's temperature and send that information directly to your computer or mobile device. Through connected kitchen appliances, you can start dinner from the office, check social media accounts from your grill or know when you're low on milk. Cyberspace is, and will increasingly be, the economic engine of the 21st century economy.

At the same time, as the Internet and information technology become increasingly entwined in our daily routines, cyberspace becomes a limitless and adaptive attack surface. The security challenges will be more diverse and harder predict. And the consequences will be more severe. We may not be able to secure cyberspace but it is our collective responsibility to understand the threat in order to minimize its effect on our privacy, civil liberties, national security and economic prosperity.

I encourage all my colleagues, on both sides of the aisle, to embrace the unique opportunity this hearing presents. We are not here to debate data breach legislation or other specific policy issues. We are privileged to have an impressive panel of experts who can help us understand the challenge of cybersecurity in context. I look forward to hearing from each of our witnesses and the unique perspectives they bring to this important discussion. In particular, I want to recognize Dr. Shannon from Carnegie Mellon University, which is home to the nation's first computer emergency response team. The Pittsburgh region boasts some of the nation's foremost experts in the field of cybersecurity, and I am pleased to have one of those experts, Dr. Shannon, joining us here today.

###