Opening Statement of Chairman Chris Collins
Subcommittee on Health and Technology
Protecting Small Businesses Against Emerging and Complex Cyber-Attacks
March 21, 2013

Good morning. I call this hearing to order.

I want to welcome our new members to the Subcommittee, especially Ranking Member Hahn. I look forward to working with you, and all of our members during the 113th Congress. I also want to give special thanks to our panel of witnesses for taking time away from your fulltime jobs and making the trip to Washington for this important hearing.

Our nation's digital infrastructure has become an essential component for how small businesses operate and compete in the 21st century. It provides access to a variety of innovative tools and resources to help reduce costs and increase productivity. Email, social media, online sales, and global video conferencing are just a few examples. New innovations and capabilities are being developed every day as a result of the Internet. And this means new jobs for main-street America, and new tools for small businesses.

The rapid development in information technology is truly fascinating to watch. A couple of the most dynamic industries have been the emergence of cloud computing and mobile applications. It is now easier than ever for small businesses to store and access their information from anywhere in the world; without purchasing thousands of dollars in IT equipment.

In addition, the boom in mobile applications is a great success story for both entrepreneurs looking to create the next best app, and for the small businesses that use them. From mobile banking to online marketing, there is a plethora of applications available to help small firms increase their productivity. And considering the NCAA tournament is set to tip off any minute now, I'm sure there are some people in this Chamber who are streaming the games from an application on their mobile device.

Unfortunately, the growth of information technology has also attracted a growing number of cyber-criminals looking to steal sensitive information – including intellectual property and personal financial information. These attacks can be catastrophic, leaving many small businesses

unable to recover. A report shows that nearly 60 percent of small businesses will close within six months of a cyber-attack.

The recent string of cyber-attacks on high-profile companies is a stark reminder of the current threat. Although small businesses don't make the headlines, a recent report shows nearly 20 percent of cyber-attacks are on small firms with less than 250 employees.

Small businesses generally have fewer resources available to monitor and combat cyber threats, making them easy targets for expert criminals. In addition, many of these firms have a false sense of security and believe they are immune from a possible cyber-attack. The same report shows 77 percent of small firms believe their company is safe from a cyber-attack – even though 87 percent of those firms do not have a written security policy in place. There is clearly a gap in education and resources. Moreover, the sophistication and scope of these attacks continue to grow at a rapid pace.

A report by the Office of National Counter Intelligence Executive indicated that tens of billions of dollars in trade secrets, intellectual property, and technology are being stolen each year by foreign nations like China and Russia. These are not rogue hackers. They are foreign governments engaged in complex cyber-espionage with a mission to steal our trade secrets and intellectual property. As the leader in producing intellectual property, the United States and small businesses, will continue to be a primary target for cyber criminals seeking an economic advantage.

Protecting our digital infrastructure is complex and no one federal agency or private business can do it alone. It takes a true public-private partnership to identify, combat, and share information regarding these sophisticated cyber-attacks. As we consider new cyber-legislation, we must work to identify the correct balance between imposing new onerous regulations for small businesses and protecting our digital infrastructure.

Again, I want to thank our witnesses for participating today. I look forward to hearing how we can better assist small businesses in utilizing new technologies while protecting them against cyber-attacks.

I now yield to Ranking Member Hahn for her opening statement.