Statement Of
Rep. Mac Thornberry (TX-13)

Before The

House Committee On Small Business
Subcommittee On Healthcare and Technology
United States House Of Representatives

December 1, 2011

Chairwoman Ellmers, Ranking Member Richmond, and Members of the Subcommittee, I appreciate the opportunity to offer some thoughts today about cybersecurity.

Cybersecurity is a complex set of issues that touches nearly every aspect of our lives. It is not only about national security, but also job creation and our economy. Every day, businesses of all sizes are targeted for their intellectually property – things like blueprints, formulas, and business plans. When information is stolen from U.S. databases, jobs are stolen from the U.S. economy.

We even hear stories of small businesses developing a new product, being hacked, and finding copies of their new products hitting the market at cut-rate prices from overseas countries within a few months. This is a direct threat to our global competitiveness.

Every day most of us take common-sense precautions about our personal safety and valuables. We lock our doors; we keep our cash in a safe place; we do not give out our bank account or Social Security numbers to anyone we do not trust. Yet, too many of us do not take such precautions in one of the most dangerous places where many go every day — cyberspace.

Earlier this year, U.S. House Speaker John Boehner and Majority Leader Eric Cantor asked me to lead a Task Force to make recommendations on what Congress could do right away to deal with this problem. The goal was not to develop legislation, but to make

recommendations that provide a framework for the committees to write and pass legislation during this Congress that will make a real difference in cyber.

Part of the reason that little progress has been made is that cybersecurity is a complex issue that cuts across jurisdictions and turf in both the legislative and executive branches of government. The Task Force, made up of 12 Members representing 9 different committees and 3 at-large Members, enabled us to get past many of the jurisdictional hurdles by getting everyone in the same room to talk cybersecurity. Each committee was able to hear the different perspectives and approaches from other committees, which went a long way in gaining a better view of the challenges that we face.

The Task Force recommendations were delivered to Leadership and released publicly in early October of this year. Although there are many specific recommendations covering a variety of issues, generally there were two main areas that we felt would have the most impact on cybersecurity moving forward.

The first area the Task Force believes that Congress should act upon is to promote a series of incentives to help raise the level of cybersecurity generally and increase awareness. Estimates are that 85 percent of threats in cyberspace can be eliminated with proper cybersecurity "hygiene." Raising the awareness of cybersecurity to C-level executives and small business owners will help companies put in place the technology and good practices that are already available to reduce cyber attacks.

The second area is to address the more sophisticated attacks from large groups and state actors by increasing information sharing between the federal government and private businesses as well as getting companies to share more with each other. To allow this type of information

sharing for new and existing partnerships, we identified a series of laws that have not kept pace with advancements in technology that need to be updated. We also felt it was necessary to create an entity that is run and operated outside of government to act as a clearinghouse of information. By involving Internet Services Providers (ISPs) and plugging in the classified information of the federal government, this type of entity could move towards "active defense," where cyber attacks are blocked or quarantined before they even reach a company. This approach is similar to the 90-Day Defense Industrial Base (DIB) Pilot Program where ISPs use classified information from the federal government to help protect the networks of the DIB participants.

These recommendations and the others in the Task Force report will not solve all of the challenges we face with cybersecurity. However, they do offer a framework for us to move forward this Congress and increase cybersecurity protections for small businesses and our country.

Again, thank you for holding this hearing and allowing me to offer my thoughts.