House Permanent Select Committee on Intelligence
Chairman Mike Rogers Opening Statement
Open Hearing: Cyber Threats and Ongoing Efforts to Protect the Nation
October 4, 2011
***Remarks as Prepared**

Introduction: The House Permanent Select Committee on Intelligence meets today in open session to convene a hearing on cyber threats and ongoing efforts to protect the nation.

There are a wide range of cyber issues being debated these days. I would like to focus our discussion at today's hearing, however, on cyber information sharing, and in particular, what the Intelligence Community might be able to do to assist the private sector in defending their networks.

The Speaker has asked Congressman Mac Thornberry of this Committee to lead the efforts of the House on the broader range of important cyber security issues, and his Task Force has done some very important work in thinking through some of these difficult problems. He has the full support of the House Intelligence Committee as he does his work, and I hope this hearing will be of benefit to the work of the Task Force.

Our witnesses for today's hearing are The Honorable Michael Hayden, Mr. Arthur Coviello, and Mr. Kevin Mandia.

General Hayden has had a very long and distinguished military career. His assignments include serving as director of the National Security Agency, and director of the Central Intelligence Agency. He also served as the Principal Deputy Director of National Intelligence, and he is no stranger to the significant cyber threats we face from nation states like China.

Mr. Coviello is the Executive Chairman of RSA Corporation, a company which plays an important role in helping secure both private and government networks and systems.

RSA's business alone would probably be sufficient to qualify him to testify before the Committee on cyber, but RSA was also the target of a significant cyber attack recently, and therefore serves as a useful case study of the state of our cyber security efforts.

Mr. Kevin Mandia is the Chief Executive Officer of MANDIANT, an industry leader in cyber incident response and computer forensics. Mr. Mandia deals with the consequences of advanced cyber espionage against American companies every day, and we look forward to his observations on the threats we face, as well as what we can do to better cope with them.

The Threat
The United States faces a significant and ongoing cyber security threat today; one that presents issues of national and economic security.

There has been a lot of talk about the prospect of a "cyber-Pearl Harbor" attack that could shut down critical infrastructure and potentially cause actual physical damage in the U.S.

A potentially destructive threat against critical infrastructure is certainly possible. I am more concerned, however, about the "death by a thousand cuts" that we are suffering right now from cyber espionage being conducted every day against nearly every sector of our economy.

These cyber espionage attacks result in massive losses of private sector intellectual property and sensitive government information. Urgent action is required to staunch the bleeding.

Indeed, most businesses report they have been the target of malicious cyber activities this year, and nearly everyone who uses email or social networks has been the target, if not a victim, of fraud or hacking.

The technological leadership and national security of the United States is at risk because some of our most innovative ideas and sensitive information are being brazenly stolen. Attackers have little to fear because we have no practical deterrents.

There are also significant liability and customer trust consequences to cyber attack. The stigma associated with cyber attack makes most companies reluctant to share threat information with each other, with the government, or the public.

Without an open exchange of information about cyber threats, companies are missing an opportunity to use shared experience to learn how to defend themselves more effectively.

Mischief is no longer the primary goal of cyber intrusion. What started out as a kid in the basement hacking into a school computer to change a grade, has evolved into entire nation states focused and determined to exploit our nation's cyber systems. Organized criminals and nation states now drive industrial scale cyber espionage.

Assistance from the Intelligence Community

I would like to have a good discussion today about the advanced cyber threats we face, but just as importantly, we also need to have a good discussion about possible solutions.

The government in general, and the Intelligence Community in particular, has an important role to play in protecting its citizens and its economy from cyber crime and espionage, but we are not taking advantage of the strengths and assets they bring to the table.

The Intelligence Community collects valuable information about advanced foreign cyber threats that could dramatically assist the private sector in the defense of their networks. For a variety of legal and policy issues, however, we don't get the full value of those valuable intelligence insights. Essentially, the United States is fighting with one hand tied behind its back.

The good news is that there is some innovative work being done in the Department of Defense that suggests a way forward to changing this paradigm.

The DIB Pilot
The Department of Defense has introduced a set of programs that helps enable defense industrial base (or "DIB") companies protect themselves by providing them with cyber threat intelligence.

These DoD efforts include a pilot program in which trusted internet service providers use classified information to help protect DIB companies that voluntarily request such assistance.

Initial results for these programs are positive. We must refine and expand these kinds of innovative efforts so they can help protect the broader government and private economy.

Besides providing actionable government information to the private sector, we need to think about how the private sector, which owns the vast majority of the cyber infrastructure, can voluntarily provide privacy protected information to the government to help the government do a better job on cybersecurity.

Chinese Economic Cyber Espionage
I would like to conclude this morning with a few words about pervasive Chinese economic cyber espionage.

There is a rich history over the centuries of governments and militaries conducting espionage on each other to better understand each other's plans, intentions and capabilities. It would, of course, be odd for me to lament these efforts, from my position as Chairman of the House Intelligence Committee.

These espionage activities over the years, however, have largely been focused on collecting intelligence on foreign governments and militaries, not on brazen and wide-scale theft of intellectual property from foreign commercial competitors.

You don't have to look far these days to find a press report about another firm, like Google, whose networks have been penetrated by Chinese cyber espionage and have lost valuable corporate intellectual property.

And that's just the tip of the iceberg. There are more companies that have been hit that won't talk about it in the press, for fear of provoking further Chinese attacks.

When you talk to these companies behind closed doors, however, they describe attacks that originate in China, and have a level of sophistication and are clearly supported by a level of resources that can only be a nation-state entity.

Attributing this espionage isn't easy, but talk to any private sector cyber analyst, and they will tell you there is little doubt that this is a massive campaign being conducted by the Chinese government.

I don't believe that there is a precedent in history for such a massive and sustained intelligence effort by a government to blatantly steal commercial data and intellectual property.

China's economic espionage has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy.

Beijing is waging a massive trade war on us all, and we should band together to pressure them to stop. Combined, the United States and our allies in Europe and Asia have significant diplomatic and economic leverage over China, and we should use this to our advantage to put an end to this scourge.

Conclusion
Whether or not we will ever be able to convince Beijing to voluntarily stop their dirty economic cyber espionage campaign, we have a lot of work to do here in the United States to improve our cyber security, including improving the sharing of cyber threat information within and between the government and the private sector..

General Hayden, Mr. Coviello, and Mr. Mandia are excellent resources to help us understand these issues, and I look forward to today's discussion.

General Hayden, would you like to begin?