CYBER SECUREAMERICA COALITION

The Honorable Diana DeGette
Ranking Member, Subcommittee on Oversight and Investigations
House Committee on Energy and Commerce
2322A Rayburn House Office Building
Washington, DC 20515

July 9, 2013

Dear Ranking Member DeGette:

I am writing to commend you for your leadership on the issue of cyber security and to thank you for holding the July 9th hearing entitled: Cyber Espionage and the Theft of U.S. Intellectual Property and Technology. This is a critical issue for our nation which requires strong leadership from Congress to combat this threat.

I write today as Executive Director of the Cyber Secure America Coalition, a collection of companies dedicated to pursuing positive cyber security legislation necessary to make the U.S. IT infrastructure more secure. Our Coalition members are leaders in the industry and include, Kaspersky Lab, TrendMicro, Qualys, CyberPoint, TechGuard Security and Nok Nok Labs. Combined these companies represent decades of efforts to fight cyber threats including cyber espionage and the theft of intellectual property, so critical to the competitive advantage we need in this country to innovate and promote our nation's economic well being.

In today's cyber world, the threats are real, sophisticated and coming at a more rapid pace. Gone are the days when viruses were just a form of graffiti on the Web. Today, cyber criminals in all forms are focused on stealing valuable information, whether it is credit card numbers, personal data, corporate information or classified government information. It is a much more dangerous world in cyber space. We believe that this will only continue to escalate as more and more valuable information is available in digital form.

It is easier to hide one's identity or location in the cyber world versus the physical world. Thus it becomes relatively more difficult in the cyber world to catch those that would do harm. The record shows, however, that it is possible through cooperation and effort of law enforcement at all levels, including at the international level with organizations like Interpol to catch cyber criminals. It is also clear that we need appropriate cyber crime penalties to punish those that

are apprehended. We believe that governments must send the message that cyber crime does not pay.

To effectively combat cyber espionage and intellectual property theft, the Cyber Secure America Coalition believes that there are key legislative actions that can help to protect against the cyber threats of today and beyond. It is critical that key U.S. business and government entities take steps to strengthen individual and collective cyber security and protect critical digital assets. Therefore we recommend the following actions:

1. Passage of enhanced information sharing legislation about cyber threats between the private sector and the federal government to improve cyber security. This will provide real-time actionable intelligence that will help better protect against cyber attacks. Legislation must include liability protection from lawsuits for those that share information in good faith for the purpose of improving cyber security.

2. Safe Harbors from disclosure of cyber attacks should be developed to support companies that meet certain security frameworks as an to incentive to improve baseline security. To achieve a safe harbor, companies should at least take steps along the lines of the following:

- Demonstrate continuous monitoring of enterprise security architecture through a cyber security "industry standard" regime. An example would be the "SANS 20 Critical Controls" that are widely deployed by companies that are serious about security;

- Demonstrate compliance with all relevant federal and state cyber security laws such as data breach notification and HIPAA; and

- Designate an officer of the company with responsibility and accountability for cyber security.

3. Identification of the most important aspects of the critical infrastructure and steps should be taken to better protect the integrity of those systems. This includes the development of voluntary, flexible standards for the critical infrastructure. These standards should be based on existing international standards and best practices. There should be incentives for implementation, and liability relief for those critical infrastructure industries that participate in such a voluntary program.

The Cyber Secure America Coalition is committed to being a partner in helping to better secure our national digital assets. We need to do more to combat cyber espionage and intellectual property threat. Improved cyber security in the public and private sectors can achieve that objective. No security is perfect, but we must do more to ensure that our competitive advantage remains. The US competitive advantage in e-commerce and innovation is, in the view of our member companies, critical to restoring and enabling vibrant economic growth. We look forward to working with the Subcommittee as you tackle this important issue in the months ahead.

Thank you again for your leadership.

Sincerely,

Phil Bond
Executive Director