Ranking Member Brian Higgins (D-NY) Opening Statement

Subcommittee on Counterterrorism and Intelligence

"Economic Espionage: A Foreign Intelligence Threat to American Jobs and Homeland Security"

June 28, 2012

Tom Friedman in his book, 'The World is Flat' discusses today's global, web-enabled world that allows everyone to 'plug in and play', sharing knowledge and work, irrespective of time, distance, and geography.

This paradigm makes the United States a target for economic espionage where other nations work covertly to obtain sensitive technology and economic information to undermine our status as a global economic leader. Economic espionage is not a new concept. It has posed a threat to U.S. national security for years.

But now it has now it has become an issue for American business as well. According to the Federal Bureau of Investigation, U.S. companies suffered more than $13 billion dollars in economic losses in Fiscal Year 2012 alone. That is an appalling figure, and what is more astonishing is that we cannot value the true long term cost of theft and transfer of intellectual property.

Economic espionage through cyber attacks committed by foreign intelligence services and other criminal enterprises is so pervasive that in a recent poll, 90% of companies admitted their networks had been breached in the past 12 months, while the other 10% could not say with certainty that they had not been penetrated.

According to the former White House cybersecurity advisor Richard Clarke, every major company in the United States has already been penetrated by China. The Chinese have been linked to a white range of economic espionage in recent years, including the theft of blue prints for the next generation stealth fighter from a defense contractor. Last month in a report issued by the Pentagon, officials stated China would continue to be an "aggressive and capable" collector of sensitive U.S. technological information.

Additionally, in its report to Congress, the Office of the National Counterintelligence Executive judged that the most active and persistent perpetrator of economic espionage is China. China is not the only country focused on the United States, the NCIX also named Russia as aggressive in their pursuit of U.S. trade secrets.

Further, just about two months ago, this Subcommittee also heard from witnesses that stated that our critical infrastructure was vulnerable to an attack from Iran.

Given the wealth of trade secrets in America, I am sure it could be possible for it to be vulnerable to espionage from other countries aside from these I have mentioned. Knowing these facts, the Administration is right to take steps to address economic espionage and I am looking forward learning more from the testimony today. I hope they can give us as much insight as they can in an open setting.

Although the Administration has issued these stern warnings of the threat of economic espionage in reports and through advertisements, Congress has not responded. Key legislation that would have helped protect our most sensitive industries and critical infrastructure from cyber intrusions were not even allowed to be considered by the House.

I was disappointed that the Majority's philosophy this Congress has been that enhancing information sharing between companies and with the government alone is enough to adequately protect our Nation from this threat. Right now, our cybersecurity legislation is lacking with respect to critical infrastructure, but it seems as if right now the government and companies will have to deal with the resources that are currently available. I look forward to learning how the agencies are dealing and if they are cooperating with each other to prevent the devastation of economic espionage.