**Opening Statement of the Honorable Tim Murphy**
**Subcommittee on Oversight and Investigations**
**Hearing on "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology"**
**July 9, 2013**

*(As Prepared for Delivery)*

In the last several months, there have been increasing reports of cyber espionage and its toll on U.S. businesses and the economy. In March, Thomas Donilon, the National Security Advisor to the President, addressed the issue of cyber espionage and the theft of U.S. intellectual property, or "IP," and technology, particularly by China. Mr. Donilon stated that IP and trade secrets "have moved to the forefront of our agenda…. targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China [occurs] on an unprecedented scale. The international community cannot afford to tolerate such activity from any country." In June, President Obama raised this issue with the Chinese President during a summit in California.

Just two weeks ago, the Council on Foreign Relations released a report finding that U.S. oil and natural gas operations are increasingly vulnerable to cyber attacks, and that these attacks damage the competitiveness of these companies. The victims go beyond the energy industry, though. A recent report by a cybersecurity consulting firm documented the Chinese People Liberation Army's direct involvement through cyber attacks and espionage into 141 companies, including 115 in the U.S., across 20 industries.

Three years ago, Chinese military hackers infiltrated the Pittsburgh location of QinetiQ, a manufacturer of high-tech robotic systems like the remotely-controlled devices used to diffuse IEDs. Experts believe the Chinese hackers may have stolen from QinetiQ's proprietary chip architecture, allowing the PLA to take over or defeat U.S. military robots and aerial drones.

From defense contractors to manufacturers, no American company has been immune from the scourge of Chinese intellectual property theft. In January, two Chinese citizens were convicted for attempting to steal trade secrets from a Pittsburgh Corning plant in order to build a rival factory in China.

Cyber espionage has obvious implications for national security, foreign relations, and the American economy. The Commission, which Senator Slade Gorton represents today, recently published a report on the theft of intellectual property and estimated that it costs the U.S. economy over $300 billion a year, which translates into roughly 2.1 million lost jobs. To put this in perspective, the IP Commission found that the total cost of cyber theft was comparable to the amount of U.S. exports to Asia. General Keith Alexander, the director of the National Security Agency, called cyber crime, and the resulting loss of our intellectual property and technology to our competitors, "the greatest transfer of wealth in history."

The purpose of this hearing is to understand how this loss is happening, the cost to our country, and how companies and the U.S. government are responding to this threat. The testimony of the IP Commission and the U.S.-China Commission make clear that the People's Republic of China is the most predominant and active source of cyber espionage and attacks. China, while the main source, is not the only one. The Office of the National Counterintelligence Executive (ONCIX) states Russia, too, is aggressively pursuing U.S. IP and technology.

The witnesses today will explain the methods and tactics used to penetrate U.S. cyber systems, and what China and other perpetrators do with the information they obtain through these attacks. Counterfeiting of U.S. products and technologies is often an unfortunate result of cyber espionage attacks. In an op-ed submitted to the Washington Post, Admiral Dennis Blair, former director of

national intelligence, and Jon Huntsman, Jr., the former ambassador to China, explained how the counterfeiting of a U.S. product by a foreign company resulted in the foreign company becoming the largest competitor to that U.S. company. Ultimately, the U.S. company's share price fell 90 percent in just six months.

Just last month, federal prosecutors secured an indictment against Sinovel, a Chinese wind-turbine company, for stealing source code for small industrial computers used in wind-turbines for a U.S. business, American Semiconductor Company. The CEO of American Semiconductor remarked on the reported $1 billion loss in market value his company suffered as a result of this theft, stating, "...If your ideas can be stolen without recourse, there is no reason to invest in innovation, there is no purpose to the American economy."

I would like to thank the witnesses. First, we have the Honorable Slade Gorton the former Senator from the State of Washington and currently a Commission Member on the Commission on the Theft of American Intellectual Property. Joining him is an expert on cyber security and Chinese foreign policy, the Honorable Larry M. Wortzel, Ph.D., who is a Commissioner on the U.S.-China Economic and Security Review Commission; Dr. James Lewis, Ph.D. a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS); and Susan Offutt, Chief Economist for Applied Research and Methods with the General Accountability Office.

We invited a spokesperson from the White House and the administration to join us today, but they informed the committee that they would respectfully decline its invitation. It is unfortunate that the administration did not take this opportunity to join us and testify given the importance of this issue and the priority the administration has given it during its recent talks with the Chinese President.

###