**Senator Sheldon Whitehouse**
**"Economic Espionage and Trade Secret Theft:**
**Are Our Laws Adequate for Today's Threats?"**
**May 13, 2014**
**Opening Statement as Prepared for Delivery**

Welcome to today's hearing entitled "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?" Today, this Subcommittee will explore how we can better protect American businesses from those who try to steal their valuable intellectual property.

American companies are the most innovative in the world. Companies of every size and in every industry – from manufacturing to software to biotechnology to aerospace – own large portfolios of legally protected trade secrets. In some cases, the "secret sauce" may be a company's most valuable asset. The theft of these secrets can lead to devastating consequences: for small businesses, it can be a matter of life and death.

The risk of trade secret theft has been around as long as there have been secrets to protect; there is a reason why Coca-Cola has kept its formula locked away in a vault for decades. But in recent years the methods used to steal trade secrets have become more sophisticated. Companies now must confront the reality that they are being attacked, on a daily basis, by cyber criminals who are determined to steal their intellectual property. As Attorney General Holder observed, there are two kinds of companies in America: "those that have been hacked, and those that don't know they have been hacked." Today, a criminal can steal all of the trade secrets a company owns from thousands of miles away without the company ever noticing.

Many of the cyber attacks we are seeing are the work of foreign governments. China and other nations now routinely steal from American businesses and give the secrets to their own companies. And let's be clear: we do not do the same to them. We are now going through a healthy debate about government surveillance, but there is no dispute about one thing: our spy agencies do not steal from foreign businesses to help American industry.

While cyber attacks are increasing, traditional threats remain. Company insiders walk off with trade secrets to sell to the highest bidder. Competitors steal secrets through trickery or by simply breaking into a factory or office building.

It is impossible to determine the full extent of the loss to American businesses as a result of the theft of trade secrets and other intellectual property. There have been estimates that our nation may lose anywhere from 1-3% of our GDP through trade secret theft alone. The Defense Department has said that, every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from computer networks belonging to American businesses and governments, and estimates of the value of IP stolen by foreign actors are as high as $300 billion. General Keith Alexander has characterized the cyber theft of American intellectual property as "the greatest transfer of wealth in history."

But no estimate can fully capture the real impact of trade secret theft. Because when other countries and foreign businesses steal our trade secrets, they are stealing our ideas. They are stealing our innovation. Most importantly, they are stealing our jobs.

In my own state of Rhode Island, we continue to face unacceptably high unemployment – despite having some of the most innovative businesses in the country. If we do not protect our

businesses from those who steal their intellectual property, then we are letting that innovation go to waste, and we are letting American jobs go overseas.

In the past, some companies were reluctant to talk about this issue, because no one likes to admit that they have been victimized. But many are coming forward to speak out now because they recognize how important it is that we work together to address this threat. I particularly want to thank the company representatives who are appearing before us today, as well as the many others who have working closely with me and other Senators.

I am encouraged that the Administration released a blueprint for a strategy to combat trade secret theft last year, and agencies across the government are increasing efforts to address this problem. The Administration must recognize that the theft of intellectual property is one of the most important foreign policy challenges we face, and it must communicate to China and other nations that stealing from our businesses is unacceptable.

We in Congress must do our part. We need to make sure that our criminal laws in this area are adequate and up to date. Last fall, Senator Graham and I released a discussion draft of legislation designed to clarify that state-sponsored overseas hacking could be prosecuted as economic espionage, and to strengthen criminal protection of trade secrets. We received valuable comments and suggestions about the legislation. We look forward to hearing from our witnesses today about how to improve our laws, and we hope to introduce our legislation in the coming weeks.

Companies also need civil remedies against those who steal from them. While state law has traditionally provided companies with remedies for misappropriation of trade secrets, there is currently no federal law that allows companies themselves to seek civil remedies against those who steal from them. Senators Coons and Hatch have recently introduced legislation to give victims of trade secret theft the option of pursuing thieves in federal court. Senator Flake has also introduced legislation to give companies a federal civil remedy for trade secret theft. I hope that the Judiciary Committee will act soon on legislation to strengthen both the criminal and civil protections against trade secret theft, and I look forward to working with my colleagues toward that goal.

Today, we will hear from witnesses in government, industry, and the nonprofit sector who confront the threat of trade secret theft on a daily basis. What I hope will be clear by the end of this hearing is that we need an "all-in" approach to this problem. We must strengthen our criminal laws, and our law enforcement agencies must prioritize stopping trade secret theft before it occurs and investigating and prosecuting it when it does. I will add that there remains an urgent need for us to pass broader cybersecurity legislation, and I appreciate working with Senator Graham on that effort.

I look forward to hearing from our witnesses today and to working with my colleagues on both sides of the aisle to address this critical issue.