BULLET POINTS

Overseas Security Advisory Council

Thursday, November 20th

- Open. Jokes and thank you to Peter Ford for having you and for keeping American diplomats serving all around the world in tough spots safe.
- The importance of protecting intellectual property.
- China is ravenous in stealing American intellectual property and the jobs that come with it.
- Our dependency on the internet grows with each passing day.
- As the role of technology in our lives becomes increasingly complicated and our technological dependence grows, the cyber threat from state and non-state actors grows at an even faster rate.

- It seems that hardly a day goes before I hear a story about another American company being hacked and losing valuable research and development work or other important intellectual property.
- Getting hacked seems to be all the rage in corporate America.
- It's bad and it's almost certainly going to get worse. The same vulnerabilities that countries like China are using to steal and spy can also be used to break systems or alter critical data in a time of crisis or war. Heck, the Iranians aren't even waiting for war - they are attacking our banks right now.
- American intelligence agencies like the National Security Agency have much to offer when it comes to helping American companies defend themselves from these advanced cyber threats.
- That valuable information is sometimes shared with the private sector today but the government lacks clear legal authority to grant more security clearances and share that information more widely with private sector companies.
- Congress also needs to update the law to facilitate more sharing from the private sector to the government.

- Congress also needs to update the law to allow better sharing of cyber threat information **within** the private sector, so that American companies are no longer hindered by a lack of information about what attacks other elements of the private sector are experiencing and how they are coping with those attacks.
- As we change the law to open up the aperture to allow better cyber threat information sharing, we must ensure the privacy of all American citizens is

protected, and that any information voluntarily provided to the government is properly safeguarded.

- We passed a cyber threat information sharing bill in the House by a strong bi-partisan vote of 288 to 127 last April. That bipartisan vote (92 Dems) is a clear indicator of strong consensus we have among Congress and industry, Republican and Democrat, Palo Alto and Wall Street about what needs to be done.
- The ball is in the Senate's court now.
- Certainly, Snowden's illegal disclosures have complicated the effort. We can't let a 29 year old systems administer who is a traitor to his country stand in the way of something so important to protect our economy.
- Of course, information sharing is an important tool in the cyber fight, but it is not a cure all. Companies need to bring all the tools to bear to have any hope of keeping their networks running and secure.

- Thank you for your time. I look forward to your questions.