SAMPLE SPEECH – OSAC 11/21

Thank you so much to Peter Ford for having me here today and for all of his work keeping our diplomats safe in tough spots all around the world.

Well, these days I am just happy to be anywhere. Heck, after defending the NSA's programs all summer, then the Syria mess, my own family doesn't even like me anymore.

As a matter of fact, my dad is fond of saying I got five boys, four turned out really good and I got one in Congress.

It's an honor to speak to a forum like OSAC that is so vital to promoting security cooperation between the American private sector and the U.S. government around the world.

The topic of this conference, the protection of intellectual property, couldn't be more relevant and timely. I'm sure I don't have to explain to some of the folks in this room today the lengths that countries like China will go to steal the innovation and research and development that is at the heart of America's economic strength.

Our innovation, our creativity has kept America as the top economic superpower and helped sustain our middle class, which is the envy of the world.

This isn't a completely new development, of course. The Chinese used to conduct retail operations, running human spies to infiltrate American companies to steal things like new pesticide formulas and other innovative products that their own economy can't produce.

More recently, the Chinese intelligence services have expanded into the wholesale theft of American trade secrets via an unprecedented campaign of cyber economic espionage.

It seems that hardly a week goes by that you don't hear a horror story about an American company being hacked and losing valuable research and development or other important intellectual property – and the jobs that come with it. This cyber economic espionage by countries like China steals jobs and income from American families, and it is eroding our economic prosperity.

Getting hacked seems to be all the rage in corporate America. Economic cyber espionage is now so commonplace that a company might take it personally if the Chinese are not trying to get into their network – "hey, my intellectual property is worth stealing too!"

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. These agencies collect classified information overseas about advanced foreign cyber hackers and their plans to attack the networks of American companies.

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. Voluntary information sharing with the government gives our intelligence agencies important tips and leads to help them find advanced foreign cyber hackers overseas. This in turn allows the government to provide more effective cyber threat intelligence back to the private sector to help it protect itself.

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. I believe Congress can agree to a law that facilitates more effective cyber threat sharing that also gives Americans confidence that the law won't be misused to harm their privacy and civil liberties.

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 with 92 Democrats 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. I am working with my Senate colleagues to get meaningful cyber threat information sharing legislation passed into law because at the end of the day, we are not that far apart. I remain optimistic that Senate can agree on an information sharing bill that will get us to conference, so that we can get a bill to the President's desk.

Certainly the recent illegal disclosures have hampered these efforts as people are now extra weary about giving the NSA any new ability to do anything.

But you know what?

We are going to have to dust ourselves off of this and move forward. This is as serious a threat to our economy and our way of life as there is and if we don't address it soon, China will simply have stolen all of the intellectual property the people of the United States have to steal and will march their way to a world power. I don't think that will be a good day for anyone by the way.

We can't let a 29 year old systems administrator who is a traitor to this country stand in the way of something so important to protect our economy.

My Ranking Member Dutch Ruppersberger and I worked hand in hand to pass a 40 page bill, which passed on the House floor this year with an overwhelming bipartisan vote. It's a bill that has 27 provisions to protect privacy and individual liberties. This issue is too important to let languish a minute longer. We now need the Senate to act as well so we can get this bill to the President to sign.

Thanks for being interested in this important issue, thanks for what you all do and for having me here this morning.

I’m happy to take any questions you might have.