**BULLET POINTS**

## Optical Society of America

Monday, November 18th at 2:15pm

- 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.

- Another powerful tool in that cyber fight is better encryption and more secure means of communication, both of which can be significantly improved via quantum mechanics – the place where cybersecurity and the field of optics meet.

- As I'm sure many of you know, the Holy Grail in the encryption race is quantum computing, which can be used to break the encryption we use now and to build encrypted communications that cannot be broken.

- I know that the Optical Society of America supports research in quantum computing, and that optics play an important role in the progress we are making this vital field.
- There is a long way to go before we will see quantum computing in the mainstream, but we have seen amazing progress in recent years.
- As we speak, American scientists are putting together the building blocks for quantum computing. On bench tops and tabletops we have seen experiments that have built small quantum computers.

- These experiments are very important steps toward a more secure and prosperous future for all Americans. I would like to thank all of you in the audience today who are working on the optical technology that will help enable that future.

- I am also privileged to serve on the Energy and Commerce Committee where we have jurisdiction on everything from healthcare to the Internet to energy issues. It is important work and there is a definite nexus between my two committees.

- Most recently, I have served as the co-chair of the Supply Chain Working Group. In 2012 the Intelligence committee released a report on two Chinese telecom manufacturers: Huawei and ZTE. The report brought to light the activities of the

People's Liberation Army and their intent on penetrating our networks to steal military secrets and intellectual property.

- The Working Group took a deeper dive into how vulnerable the supply chain is and how do we move forward. This is a new domain for all of us and we need to tread lightly. It's important to secure the supply chain without disrupting commerce.

- The Group has spent the last several months meeting with industry folks and is currently working on a findings report. I look forward to being able to discuss the findings.
- Thank you for your time. I look forward to your questions.