HALL OF THE STATES, SUITE 602
444 NORTH CAPITOL STREET, N.W.
WASHINGTON, D.C. 20001

PHONE: 202.624.1407
FAX: 202.624.1406
E-MAIL: contact@uscc.gov
www.uscc.gov

U.S.-CHINA ECONOMIC & SECURITY REVIEW COMMISSION

WILLIAM A. REINSCH, CHAIRMAN
DENNIS C. SHEA, VICE CHAIRMAN

Representative Tim Murphy
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6371

Dear Chairman Murphy,

I am pleased to respond to questions posed by Members of the House Energy and Commerce Oversight and Investigations Subcommittee regarding my testimony provided on July 9, 2013. These responses represent my own views and not those of the U.S.-China Economic and Security Review Commission.

Additional Questions for the Record

The Honorable Tim Murphy

1. **There has been tremendous attention recently by the Administration on this issue of cyber espionage. Statements by Secretary Lew, General Keith Alexander, and the President himself. Are they having any impact?**

   It is useful to raise public, government and corporate awareness of the threat of cyber espionage; therefore I think statements by officials such as Secretary Lew and General Alexander have some impact.

   a. **Has cyber espionage supplanted terrorism as the number one threat to this country as some in the Administration have suggested?**

      Cyber espionage costs the United States a lot of money and, in part, may be linked to network reconnaissance that later can he used in war or for cyber terrorism. However, the threat of traditional terrorism, in my view, remains high. Also, cyber espionage does not directly kill people or destroy property, while terrorism can be deadly.

2. **We hear from companies constantly that they do not want to share information about their incidents out of either fear or shame that something bad has occurred. They are especially reluctant to share an incident if it means they lose sensitive IP or technology. Is this a good approach for companies? What do they have to gain by not reporting this information?**

In the long run, companies might do better if they came to some common agreement to disclose incidents. However, I am sure that individual corporate counsel and boards will set policies that they believe are best for the corporations. By not reporting information, companies do not face a potential loss of consumer confidence, lower public opinion about the brand, or a potential loss of stock value.

a. Are U.S. companies fearful that if they report this type of information they will lose market share or future business in China?

In meetings in China with US companies and with officers of the American Chamber of Commerce, commissioners have been told privately by many corporate representatives that one reason they hesitate to complain about Chinese cyber activity and about intellectual property theft is that they fear that the Chinese government will retaliate against the company.

3. What is our biggest leverage against the Chinese for their acts of cyber espionage?

The biggest leverage we have against any country for acts of cyber espionage is to prosecute perpetrators for criminal activity and to sanction governments, individuals and companies that engage in intellectual property theft.

a. What role do companies have in protecting themselves?

Companies are responsible for their own protection. If companies are part of a government program, like the defense industrial security program, the government can and should set standards for protecting information. As I said in my testimony at the hearing, however, when the aggregate of economic damage from cyber espionage is as great as we see, I think President Obama can use the powers he has under the International Economic Emergency Powers Enhancement Act to sanction companies, individuals and countries that engage in this cyber espionage.

b. Are other countries raising the issue of cyber espionage with China through diplomatic channels?

Australia, Germany, Canada, the United Kingdom, and India, according to their own press, have raised the issue with China in diplomatic channels.

4. Can you explain how information or data obtained through cyber espionage is used to reduce costs/gain advantage for Chinese companies and negatively impact the U.S. economy?

As I explained in my written testimony, Chinese companies can leap-frog ahead in technologies or products that they are unable to develop independently by stealing intellectual property; they can save money, time and human capital on

research and development; and they can move right from theft to the production of goods without spending time or money on product development. Also, companies that steal intellectual property in China may benefit from government subsidies and from government procurement programs, which save them money and ensures a market for products.

5. **China is pursuing a comprehensive long-term strategy to modernize its military and investing in ways to overcome the U.S. military advantage. Cyber espionage is regarded as the greatest tool in that effort, as the Pentagon noted this May in a report to Congress on China. In that report, for the first time, the Pentagon specifically named the Chinese government and military as the culprit behind intrusions into government and other computer systems. Is this a bell-weather moment for U.S.-China relations?**

   No, I do not think naming the Chinese government and military as the perpetrator of cyber espionage is a bell-weather moment for U.S.-China relations. The Executive Branch and Congress complain all the time to Chinese officials about different practices in China. Most often, these complaints have no effect on Chinese policy. Taking action against China for this through legislation, executive order, or action by Congress to revoke permanent normal trade relations for China would be a bell-weather moment in U.S.-China relations.

6. **In your testimony, you recommend that the United States link Chinese economic espionage to "trade restrictions and bilateral issues." How would these restrictions fit within the regime of the World Trade Organization (WTO)? Could the WTO be used as a forum for addressing some of these issues?**

   There are existing provisions in U.S. law, for example, Section 337 of the Trade Act of 1930 that provide some ability to address products that result from violations of intellectual property. The utility of existing provisions in U.S. law should be thoroughly examined and steps might be taken to update and reform these laws to enhance their utility. The WTO could be a forum for addressing some of these issues, but its utility is often limited by a time-consuming and cumbersome process. Updating its rules, with the failure of the ongoing Doha Round of negotiations appears to be limited and is also constrained by the consensus-nature of decision-making. But, every avenue should be examined to address this critical area.

7. **In your testimony, you recommend that the US government, military, and cleared defense contractors implement measures such as "meta-tagging, watermarking, and beaconing." What would these measures do to improve or protect against cyber theft or espionage? Why aren't these measures already in place?**

   Meta-tags could be effective in identifying pirated or stolen intellectual property; however, actions like meta-tagging or watermarking alone are not enough. To be effective, there must be modern laws that would allow for criminal or civil action against violators. I don't believe our intellectual property protection and

economic espionage laws have kept up with the technology. Beaconing would help locate the violator and find where the stolen intellectual property resides. I don't know why such measures are not already in place. That question would have to be directed to software designers and the community of attorneys who work with them. If such measures were in place, however, there would have to be criminal or civil laws that would permit companies to go after thieves.

8. **In your testimony, you recommend that the United States government "prohibit Chinese firms using stolen US intellectual property from accessing US financial markets." Have you raised this recommendation with the Administration? What was the response? Given China's significant role in US financial markets (including the market for US Treasuries), do you see the potential for retaliation? Why or why not? Do the potential benefits of such a policy outweigh the potential effects of retaliatory measures?**

The Commission is a body established by Congress to report to Congress. I have not raised these matters with the administration. However, I note that up to this point, no U.S. Trade Representative has sent a panelist or witness to any of the Commission's hearings when they have been invited to do so. China invests in the U.S. for its own purposes.

In my view, it would be a good thing if equity investments by China were reduced. As for securities, the Commission's hearings on Wall Street have convinced me that China's investments in U.S. securities are a small part of the total U.S. bond market. If China moved that money all at once, there might be a slight effect on interest rates, but where would they put the money that is as secure? Most bankers that have testified before the Commission think this is an idle threat.

9. **As evident at the recent summit between President Obama and President Xi Jinping of China, diplomatic talks on the issue of cyber security have been relatively ineffective at addressing this issue. What steps, do you believe, would be more effective at addressing these state-sponsored attacks?**

The President should use his executive powers to sanction companies and individuals in China that engage in this massive cyber espionage. Also our criminal and civil laws should be reviewed and updated to ensure that action can be taken against violators.

<u>The Honorable Cory Gardner</u>

1. **In the energy sector, protecting intellectual property is less tangible than other industries, and arguably more difficult to address. Keeping in mind the complexities on legislation in this space, as all industries are different and cyber does not have neat borders, what more could be done apart from the President's recent Executive Order to prevent these types of attacks?**

The government can help industry in all sectors with information on best practices and with security measures. Congress can pass legislation that has strong criminal penalties for engaging in these activities.

2. **Do you believe that allowing private industry to decide how to best secure their system – by allowing them to choose amongst the Executive Order, NIST framework, other standards, or best practices – is a workable system to gather the necessary information to combat cyber threats?**

   No, I think that in the case of intra-state critical infrastructure, the states must decide what parts of the energy industry are critical and they must set minimum standards that protect the citizens of the state from the catastrophic loss of that infrastructure to cyber-attack. In the case of inter-state critical infrastructure, when the loss of one section might have cascading, catastrophic effects on other states or the nation, the federal government must set minimum standards that industries must meet. For private companies that are not part of the defense industrial security program and are not part of the infrastructure critical to the nation, the government can provide help, and those industries can pick and choose in ways that they feel mitigate their risk in the most cost-effective way.

3. **In your opinion, do you believe that various private industries have been adequately working together to address cyber espionage and its threats as opposed to simply relying on the federal government to do it for them?**

   I think some industries have worked very hard on the problem and may be ahead of the federal government in some areas. How much they work together probably depends on proprietary matters, cost, and competitiveness, among other things.

4. **What role do private industries play in protecting their own property?**

   Private industries and citizens have the main role in protecting their own property. It is up to government to provide them an adequate legal framework to do so, to provide adequate law enforcement, and to ensure that the measures people and companies take to protect their own property do not employ illegal or excessive force, brutality, or destructive measures. These are basic public policy matters.

5. **How critical is it in legislation or any other cyber guidelines to address the importance of improving the flow of threats information sharing from all directions (such as company to company, government to company, and company to government)?**

   Legislation could require government agencies to establish specific programs to help with information sharing. But outside of national critical infrastructure and

defense-related programs, I think it is not possible to require information sharing. Nor would it be easy to verify compliance with information sharing requirements.

The Honorable Paul D. Tonko

1. **Companies know they risk their IP in China but are willing to accept that risk for the short-term economic benefits. If Chinese companies demonstrate an ability to absorb and recreate U.S. technology at quicker rates, do you foresee the costs of IP loss causing companies to reconsider where they do business?**

   Companies make their own decisions on how much risk their company can tolerate, how to mitigate that risk, and will decide on risk versus gain in China. Some may sacrifice intellectual property for market access or market share. Regardless of the outcome, corporations should be informed of the government's assessment of risk and they should have to live with the results of their decisions without relying on some government bailout.

2. **Can you express your views about the ways and means we currently investigate and sanction those that conduct IP theft? How can our methods be improved today? What new authorities can be offered to improve our methods in the future?**

   From what I have seen so far, the fusion centers involving multiple agencies of government are doing a decent job of identifying threats. I do not believe that there is an adequate structure to investigate intellectual property theft, and it would be up to Congress to define and fund such a structure. As for new authorities, I suggested a few in my written and oral testimony. Action like meta-tagging and watermarking could be effective in identifying pirated or stolen intellectual property; however, actions like meta-tagging or watermarking alone are not enough. To be effective, there must be modern laws that would allow for criminal or civil action against violators. I don't believe our intellectual property protection and economic espionage laws have kept up with the technology. Beaconing would help locate the violator and find where the stolen intellectual property resides. I don't know why such measures are not already in place. That question would have to be directed to software designers and the community of attorneys who work with them. If such measures were in place, however, there would have to be criminal or civil laws that would permit companies to go after thieves.

Member Requests for the Record

During the hearing, Members asked you to provide additional information for the record and you indicated that you would provide that information. For your convenience, descriptions of the requested information based on the relevant excerpts from the hearing transcript regarding these requests are provided below.

The Honorable Michael C. Burgess

1. **You testified that you have had success with regards to the bilateral credit card and bank crime prevention. In order to protect the smaller banks, is there a way to involve the larger offshore banks that are doing these offshore transactions?**

   From meetings with Federal Bureau of Investigation legal attaches and Department of Treasury representatives in Hong Kong and China, my understanding is that Chinese security authorities have been relatively helpful in pursuing criminal cases related to banking and credit card theft. These U.S. officials did not qualify their remarks by saying whether the cooperation is limited only to large banks or how responsive Chinese authorities are to criminal cases involving small banks. This question is best directed to the Departments of Justice and Treasury. The Internal Revenue Service also is involved in identifying and regulating offshore banking practices; IRS also may be able to respond to this question.

Thank you for the opportunity to respond to these questions. If I can be of any assistance in matters regarding cyber-security and the theft of American intellectual property please contact me.

Sincerely,

Larry M. Wortzel

Larry M. Wortzel, Ph.D.
Commissioner