FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

July 25, 2013

Dr. Larry Wortzel
Commissioner
U.S.-China Economic and Security Review Commission
444 North Capitol Street, N.W., Suite 602
Washington, D.C. 20001

Dear Dr. Wortzel:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, July 9, 2013, to testify at the hearing entitled "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

Also attached are Member requests made during the hearing. The format of your responses to these requests should follow the same format as your responses to the additional questions for the record.

To facilitate the printing of the hearing record, please respond to these questions and requests by the close of business on Thursday, August 8, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at **brittany.havens@mail.house.gov** and mailed to Brittany Havens, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations
Attachments

Attachment 1—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?

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

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?

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

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

    a. What role do companies have in protecting themselves?

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

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?

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?

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?

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?

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 Honorable Cory Gardner

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?

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?

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?

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

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)?

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?

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?

Attachment 2—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 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?