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

Mr. James A. Lewis
Director and Senior Fellow
Technology and Public Policy Program
Center for Strategic and International Studies
1800 K Street, N.W.
Washington, D.C. 20006

Dear Mr. Lewis:

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. How do you protect the designs (or blueprints) for technology developed in the United States through the production phase in China without risking it being stolen?

2. What are some common tactics used by China and the PLA to steal IP or technology?

    a. What is the PLA's assessment of US industries' ability to identify these tactics and protect against them?

    b. Have tactics changed/evolved in recent years/months?

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. What needs to change in China for them to stop their policy of cyber espionage towards our companies?

5. States actors in China such as the PLA are primarily interested in profit. In your testimony, you raise a very interesting point about the domestic costs of clamping down on cyber espionage by President Xi. What is the political climate in China that breeds the type of behavior of cyber espionage? How can these costs be reduced, and what can the international community do to raise the international costs of *not* clamping down?

6. There are currently many government agencies whose jurisdiction includes cyber security issues. Do you believe that the regulatory structure could be streamlined to address persistent cyber security threats more effectively? If so, what are your recommendations for doing so?

7. Many of China's universities offer programs in cyber security. Do you believe that similar programs should be available in the United States? How should these initiatives be developed? Is there more that U.S. universities could be doing?

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. Mr. Lewis, you present an interesting conundrum, where China's reliance on cyber espionage has undermined its ability to innovate. Do you believe this trend will continue? Will China's weak IP protections increase the likelihood that the next generation of technology will be developed and manufactured in the U.S.?

2. 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?

3. 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. When I asked you what small business can do to improve their ability to prevent, identify and mitigate the consequences of a compromise? Please elaborate on the strategies that were put in place by the Australian government to have an 85% success rate in preventing a security compromise.