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

The Honorable Slade Gorton
Commissioner
Commission on the Theft of American Intellectual Property
1414 N.E. 42nd Street, Suite 300
Seattle, WA 98105

Dear Senator Gorton:

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.

To facilitate the printing of the hearing record, please respond to these questions 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
Chairman
Subcommittee on Oversight and Investigations

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

Attachment

Attachment—Additional Questions for the Record

The Honorable Tim Murphy

1. Based on recent examples, can you reasonably itemize the costs – both tangible and intangible – that result from IP theft? For example, are there increased countermeasure costs or mitigation costs, loss of reputation or market share, or lost future R&D investments.

    a. Does the cyber element change or magnify these losses when compared to traditional corporate espionage? Make it more difficult for companies to recover? Is it difficult for companies to even know they are/were attacked?

2. The IP Commission's report raises some interesting issues relating to the loss of IP and technology in terms of dollars and jobs. If IP were to receive the same protection overseas that it does here, is it possible that the U.S. economy would add millions of jobs?

3. What kinds of protections are we missing in the U.S.?

4. When innovation is in the United States and production is overseas, how does a global market place weaken the situation for American companies?

5. Do other countries have better protections against IP theft relating to state-sponsored cyber espionage?

6. Your report recommends quicker seizure at the border by Commerce/border agents. Does this apply only to counterfeit goods coming into the US? Are we losing the market share on goods that are sold only domestically or is the lose market share on an international scale?

7. In your testimony, you highlight the importance of changing the "internal incentive structure within China." What do you mean by this? What actions are necessary to initiate this transformation?

8. 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. It is unavoidable that the digital age creates more opportunities for IP theft. But Senator Gorton's testimony states much of today's IP theft utilizes traditional economic espionage tactics – employees illegally share proprietary information; products are dissected, re-engineered, and sold without permission; digitized products are pirated and sold illegally. And many examples from the GAO reports do not involve hacking but rather IP theft by companies' own employees. I think this is an interesting and important distinction. How are the policy prescriptions for battling "old fashioned" corporate espionage in the digital age different from state-sponsored cyberattacks or hacking?

2. Cyber intrusion, particularly concerning the loss of Defense Department R&D, is a major and legitimate concern, but has hacking been overemphasized in terms of IP theft? Do other "old fashioned" means of IP theft deserve greater attention?

3. 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?

4. The IP Commission Report recommends the Secretary of Commerce be given new authorities and resources to address IP protection issues. The Department of Justice has prosecuted individual employees of American companies who have been caught attempting to carry trade secrets with them to foreign companies and entities, and other international disputes have been brought before the World Trade Organization. How do you foresee new authorities interacting with the FBI's criminal investigative division for cyber crimes and existing trade offices?

5. 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?