Response to Questions for the Record

The Honorable Slade Gorton
Former U.S. Senator from Washington State
Commission Member
Commission on Theft of American Intellectual Property

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 counter measure costs or mitigation costs, loss of reputation or market share costs, or lost future R&D investments?*

   It is difficult, if not impossible, to quantify the exact monetary loss of IP infringement. This is primarily due to companies choosing not to report loss. However, many of the losses you mentioned are real. When a company's IP is infringed upon, or stolen, the direct loss is in loss of revenue. However, this loss of revenue leads to many secondary losses including reduced budgets for R&D investments, a transfer of resources to IP protection programs (better firewalls, new internal security protocols, etc.) and away from IP creation programs, and an overall reduced incentive to innovate. If your goods and ideas are regularly being stolen, why would you spend millions of dollars to create new ones? All of these losses translate into the most tangible loss of all, lost jobs to the American workers.

   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?*

      While it is true that the rise of personal computing has added a new dynamic to protecting intellectual property, it is important to remember that nearly all IP loss, no matter how high-tech, still requires a human component. It is rare that a significant violation is perpetrated through cyber methods alone. In order for IP theft to be successful, a human element is needed. While cyber methods add new challenges, the fight is still human. The rise of cyber theft has created a new front on which companies and individuals need to protect themselves, which does cost more, but the core of why IP is being stolen remains independent of cyber methods. Cyber is just one tool. While cyber increases cost to the American economy, sometimes substantially, it is not the root of the problem.

      Yes, sometimes companies do not know they have been attacked. Most large corporations have to capacity to detect cyber attacks but many medium-sized and startup companies do have the highest network protections. When cyber attacks are mixed with traditional economic espionage elements, these small-medium

sized companies may never know their ideas have been stolen until their products show up in the market.

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 protections overseas that it does here, is it possible that the U.S. economy would add millions of jobs?*

   Yes. If fact, the U.S.I.T.C. estimated in their 2011 report that if IPR protection in China improved substantially, U.S. employment could increase by 2.1 million jobs.

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

   Protective measures can only get us so far. Policy responses to the problem of IP theft must, of course, start with defensive measures here at home, to protect what we have, but this is not nearly enough. I believe that in order substantially to solve the problem, there needs to be an internal incentive structure *within China* that creates a Chinese constituency that advocates for stronger IP protections. Until there exists in China an interest group in favor of eliminating IP theft, we are likely to see little progress. The creation of those internal groups is perhaps the only road to long term success. Purely defensive measures will likely just create better, more sophisticated thieves.

4. *When innovation is in the United States and production overseas, how does a global marketplace weaken the situation for the United States?*

   With the manufacturing process spread overseas, across multiple countries, and involving many different suppliers, one of the greatest difficulties is in ensuring supply chain accountability. Many producers, including some within the United States, are unintentionally benefiting from stolen or misappropriated IP because one of its suppliers, many steps removed, had stolen the IP. When manufacturers use these IP-violating suppliers, we just encourage that behavior. Ensuring supply chain accountability is one of the greatest challenges in a globalized manufacturing process.

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

   All countries are trying to deal with the new challenge of cyber security. Many other countries don't feel the economic losses as strongly as the U.S. because their economies aren't as dependent on innovation and IP for continued growth, such as economies built on the manufacturing of others' products. Some countries have taken a more authoritarian approach to cyber security by highly censoring the internet and tightly controlling the flow of information. We are in a difficult position of wanting to protect IP while maintaining a free and open internet, which is in itself a great source of economic growth. I believe we can do both. The U.S. is at the forefront of cyber security and many companies in the US utilize state-of-the-art systems when it comes to cyber defense. At this time, though, even this is insufficient.

6. *Your report recommends quicker seizure at the border by Commerce/border agents. Does this apply only to counterfeit goods coming into the U.S.? Are we loosing the market share on goods that are sold domestically or is loss if market share on an international level?*

   The recommendation simply aims to expedite a process that is already in place. Currently, border patrol can seize IP infringing goods at the border, but it takes a substantial burden of proof and many months of hearings, during which the goods are sold. Additionally, the recommendation aims to limit the import of goods that are created by IP infringing methods. The greatest tool the United States has to wield is our large market that IP infringers want access to. If we can find ways to limit their access to our market, perhaps we can change the incentive structure.

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?*

   Currently, those who steal or misappropriate intellectual property, especially those who live elsewhere, have little or no incentive not to steal because there are no consequences. By restricting access to our market, our greatest asset, to those who infringe on our IP, we can create advocates in China who will work for stronger IP protections. We made recommendations to do so including an expedited seizure process at the border and restrictions on the use of our financial system. These would get us started. However, there is another idea, discussed in detail in chapter 14 of our report, to impose a tariff against countries who rampantly steal IP. The Commission was not prepared to make such a recommendation because of the difficulty of estimating the value of stolen IP, the difficulty of identifying the appropriate imports, and the many legal questions raised by such an action under the United States' WTO obligations. I, however, personally support this idea and believe it should be thoroughly examined.

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?*

   Again, while diplomatic talks are important, China and other countries will only change their behavior when it is in their best interest to do so. We need to change the calculus within China.

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 have neat borders,*

what more would be done apart from the President's recent executive order to prevent these types of attacks?

We agree that every industry and sector faces a wide variety of challenges and that is why our commission took the broadest view possible when considering "IP." We consider trade secrets and proprietary processes to be IP worth protecting. For instance, when an international energy company bids on drilling on contracts, the price a competitor will bid is a highly valued secret. This number could be obtained through cyber espionage practices. Our current cyber policies are completely defensive in nature and provide no disincentive to stop hacking. Changing policies to provide incentives to stop could help deter hacking and IP theft across all sectors.

2. *Do you believe that allowing private industry to decide how to best secure their system – by allowing that 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?*

   Ensuring that every company is operating under the highest standards of cyber security is the first step in preventing cyber theft. However, even the highest private standards only employ a defensive approach which, with enough time and resources, a sophisticated hacker can overcome. We advocate a public-private partnership where private companies employ best practices to defend their IP and the government acts as their advocate, working to protect their IP overseas.

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?*

   Most of the IP intensive firms and companies are employing best practices. It is in their best interest to do so and they know that. Some of the smaller companies, especially high-tech startups and private entrepreneurs, have a more difficult time with the cyber aspect because of the high cost associated with employing best practices. But these best practices, when fully employed, are only part of the solution because, under current law, companies can only use defensive measures. Defensive tactics can stop attacks for a while, and may even stop novice attackers permanently, but sophisticated and well-resourced hackers can overcome these measures given enough time. Additionally, most of the time, their access comes through some form of human error on the party of the company, e.g. opening a phishing email that looks legitimate. Best practices can only protect for so long.

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

   Private companies are the first line of defense and the most important. Where the government can step in is in enacting policies that make IP theft less lucrative to begin with.

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)?*

   Adequate information sharing is vital at all levels. Each of the groups you mentioned has access to, and is the first to see, different information that can be used to identify, source, stop, and deter cyber attacks. Each of these groups needs to be able to share this information with each other in order to actively defend their networks.

The Honorable Paul D. Tonko

1. *It is unavoidable that the digital age creates more opportunities for IP theft. But Senator Gorton's testimony state 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?*

   The policy prescriptions are similar in many ways but the practical implementation is quite different. The policy proposals we are advocating in our report are ways to address IP theft generally, which includes both traditional economic espionage and cyber espionage. Our major conclusion is that foreign countries and companies are not incentivized away from trying to steal IP by either method. We are trying to change the calculus and make IP violations more costly for the violators.

   Practically, the digital revolution has created a new arena that companies need to defend. Today, in addition to long standing practices to combat traditional economic espionage (such as background checks on employees), companies need to actively monitor their networks, provide real-time defense, and provide increased employee training in order to prevent IP loss via cyber espionage.

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

   Studying cyber espionage, and looking for solutions, is important because cyber is a new method of stealing IP, but it is only one method, and it needs to be considered in its broad context. While it is true that the rise of personal computing has added a new dynamic to protecting intellectual property, it is important to remember that nearly all IP loss, no matter how high-tech, still requires a human component. It is rare that a significant violation is perpetrated through cyber methods alone. In order for IP theft to be

successful, a human element is needed. While cyber methods add new challenges, the fight is still human.

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?*

   I think it is unlikely that a company will decide to completely stop doing business with China. The Chinese market of over a billion people is just too lucrative. However, while they continue to trade with China, the lost revenues, the lost R&D investment, the lost incentive to innovate, and the increased expenditures on IP protection will continue to hurt the U.S. economy.

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 authorizes interacting with the FBI's criminal investigative division for cyber crimes and existing trade offices?*

   We did recommend that the Commerce Secretary be the principal government official responsible for enhancing and implementing policies regarding the protection of intellectual property, enforcement of implementation actions, and policy development. However, this in no way should be interpreted as reducing the authority of other departments. In fact, we also recommended that Congress increase Department of Justice and FBI resources to investigate and prosecute cases of trade-secret theft, especially those enabled by cyber means.

   Additionally, while the WTO can be a useful tool for resolving disputes, its dispute mechanisms have several problems. Chief among these is the time required to reach a resolution. The process can be so time-consuming that recapturing any damages through this process is often illusory. As noted in our report, many products today, especially in the software and other high-tech industries, generate the bulk of profits for their companies in the first weeks or months of release. The current WTO procedures just take too long.

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?*

   The primary way we can improve the way we deal with IP theft is to shift the cost to the IP infringers. Right now, we can delay many of the cyber attacks through best practices and we can occasionally prosecute an individual who is stealing trade secrets for a foreign country. But these types of defenses are limited and don't provide any real

incentives for the people behind the IP theft to stop. We need to create structures within China and other countries that make IP theft costly. If we do, those who have to pay this cost will be advocates for stronger IP protections and will work to ensure lasting change.