THE

IP COMMISSION

THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY

June 25, 2013
Testimony of former U.S. Senator Slade Gorton (R-WA),
Member, The Commission on the Theft of American Intellectual Property (IP Commission)
Before the Congressional - Executive Commission on China

Over the past year, I have served as a member on the Commission on the Theft of American Intellectual Property. The Commission, co-chaired by Governor Jon Huntsman, the former U.S. Ambassador to China, and Admiral Dennis Blair, the former Director of National Intelligence, is an independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academe, and politics. The three purposes of the Commission are to: (1) document and assess the causes, scale, and other major dimensions of international intellectual property theft as they affect the United States; (2) document and assess the role of China in international intellectual property theft; and (3) propose appropriate U.S. policy responses that would mitigate ongoing and future damage and obtain greater enforcement of intellectual property rights by China and other infringers.

What we found during our research and due diligence was quite alarming but not all that surprising. Our findings suggest that the value of the total loss of American IP overseas to be over $300 billion per year, comparable to the current annual level of U.S. exports to Asia. Furthermore, we estimate that China is roughly 50%-80% of the problem. Most tangibly, one study suggests that if China had the same level of IP protection as the U.S. or the U.K., there would be an increase of 2.2 million new jobs within the United States. Intellectual property rights are violated in a number of ways including violating copyright and trademark protections, infringing on patents, and stealing trade secrets. Trade secrets are stolen primarily through cyber espionage, or through traditional industrial and economic espionage.

Cyber theft is one of the main avenues by which these ideas are stolen. While hackers stealing trade secrets, money, and personal information are a worldwide problem, quantitatively, China stands out in regard to attacks for IP. A confluence of factors, from government priorities to an underdeveloped legal system, causes China to be a massive source of cyber-enabled IP theft. Much of this theft stems from the undirected, uncoordinated actions of Chinese citizens and entities who see within a permissive domestic legal environment an opportunity to advance their own commercial interests. With rare penalties for offenders and large profits to be gained, Chinese businesses thrive on stolen technology.

While our topic today is Chinese hackers and commercial rule of law, it is important to remember that cyber espionage is only part of the problem. The stories that most people hear or imagine when thinking about IP theft, economic espionage, or trade-secret theft are the grist of high-tech espionage thrillers. The mention of global IP thieves often conjures up images of a foreign enemy based somewhere on the other side of a vast ocean. State-sponsored efforts immediately leap to mind—for example, Shanghai-based PLA Unit 61398, which has been

identified as the source of many recent cyber attacks. However, 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. Much of today's IP theft still utilizes traditional economic espionage tactics. This is the apparent situation in the recent NYU case, where a Chinese government institution bribed researchers to disclose their valuable findings.

Industrial espionage is nothing new. It is a classic business tactic used by less than reputable organizations to try and obtain a competitor's secrets in order to gain an economic advantage in the marketplace. So, while members of Congress continue to work on solving the issue of cyber theft and Chinese hacking, we would encourage them to consider expanding policy proposals beyond cyber theft to international IP theft, generally.

Policy responses to the problem of IP theft must start with defensive measures here at home, to protect what we have, but this is not nearly enough. I believe that until there is a change in the internal incentive structure within China, or until there exists in China an interest group in favor of eliminating IP theft, we will likely see little progress. This is perhaps the only road to long term success. Purely defensive measures will likely just create better, more sophisticated thieves.

Along with my testimony today, I am submitting a copy of the IP Commission's report that was released May 22, 2013. The final chapters lay out a series of policy recommendations, organized as short, medium, and long-term recommendations. The recommendations vary and would likely fall under the jurisdiction of a number of Congressional committees including the Senate Banking and House Foreign Affairs Committees. The short-term recommendations suggest changing the way the U.S. government is internally organized to address IP theft and suggest new tools to create incentives overseas. These include allowing for targeted financial sanctions and quick response measures for seizing IP infringing goods at the border. The medium-term solutions suggest, among other things, amending the Economic Espionage Act and shifting the diplomatic priorities of our overseas attachés. Our long term solutions focus largely on continuing to work on establishing stronger rule of law in China and other IP infringing countries. Additionally, we offer a set of cyber recommendations that this commission will likely find interesting given the topic of today.

It is our hope that this report will help to inform and strengthen the policy changes that come from Congress and the Administration. Thank you.