THE COMMITTEE ON ENERGY AND COMMERCE

Memorandum

July 3, 2013

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing on "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology"

On July 9, 2013, at 10:15 a.m. in room 2123 of the Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology." The hearing will examine the steps taken by the federal government and the private sector to identify and mitigate the effects of cyber espionage on American companies. Testimony from experts will focus on cyber espionage, intellectual property, technology and international relations.

I. WITNESSES

Panel I

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

Honorable Larry M. Wortzel, Ph.D.
Commissioner
U.S.- China Economic and Security Review
Commission

Mr. James A. Lewis
Director and Senior Fellow, Technology and
Public Policy Program
Center for Strategic and International Studies

Ms. Susan Offutt
Chief Economist, Applied Research and
Methods
Government Accountability Office

II. BACKGROUND

The nation faces an evolving and persistent array of cyber-based threats. The sources of these threats include criminal groups, hackers, terrorists, insiders, foreign nations, or espionage and information warfare. The threat technique and magnitude grows increasingly sophisticated and in many cases targets sensitive personal or proprietary information and technology. Experts estimate that there has been a massive transfer of technology and wealth from developed

economies to developing economies. The loss of industrial information and intellectual property through cyber espionage constitutes the "greatest transfer of wealth in history," according to Gen. Keith Alexander, director of the National Security Agency and commander of U.S. Cyber Command.[1] The size and scope of the problem, while difficult to estimate because victims tend to under report occurrences, is increasing.[2]

Multiple federal agencies undertake a wide range of activities to protect of intellectual property (IP) rights. These agencies include the Departments of Commerce, Justice, and Homeland Security. For example, components within the Justice Department and the Federal Bureau of Investigation are dedicated to fighting computer-based threats to IP.

The threat of cyber espionage is not new. What is new are the methods and tactics that entities employ. The increasing dependency upon information technology systems and networked operations pervades nearly every aspect of our society. While the benefits are obvious, this dependence creates vulnerabilities that can be exploited.[3] Cyber-attacks are increasingly the method that threat actors—whether nations, companies, or criminals—use to target IP and other sensitive information and technology. According to the Office of the National Counterintelligence Executive, sensitive U.S. economic information and technology are targeted by intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries.[4]

Cyber espionage is one of the most pressing threats the nation faces. Recent reports have stated "that cyber attacks and cyber espionage had supplanted terrorism as the top security threat facing the United States."[5] For example, American oil and gas firms are frequently targeted and subject to theft of trade secret, business plans, exploration bids and geological data.[6] The loss of IP and technology poses a threat to national security not only to our military advantage (in the context of military design plans and strategies) but to our economic competitiveness. State-sponsored cyber espionage is the most harmful to U.S. IP and technology. State-sponsored opponents are the most sophisticated and have demonstrated the capacity to exploit our commercial and government networks.

---

[1] *See remarks* American Enterprise Institute event entitled "Cybersecurity and American power Addressing new threats to America's economy and military;" July 9, 2012.
[2] *See Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*; Published May 6, 2013; http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf. The report stated that cyber exploitations into U.S. government computer systems appeared to be directly attributable to the Chinese government and military. This is the first time the Defense Department has made this claim in its annual report confirming that the new level of cyber espionage is to acquire advanced technologies for military modernization.
[3] *See Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* (February 2013); http://www.gao.gov/assets/660/652170.pdf.
[4] See *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (October 2011); http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.
[5] *See* "U.S. to press China on cyber theft: Lew:" *Reuters*; Poornima Gupta; July 1, 2013, at http://www.reuters.com/article/2013/07/01/us-treasury-china-idUSBRE96009X20130701.
[6] *See generally* "*CFR Energy Brief: Addressing Cyber Threats to Oil and Gas Suppliers*;" Blake Clayton and Adam Segal; June 2013; http://www.cfr.org/cybersecurity/addressing-cyber-threats-oil-gas-suppliers/p30977.

Private sector organizations have experienced a wide range of incidents involving data loss or theft, economic loss, computer intrusions, and privacy breaches. The following examples from public sources are by no means exhaustive but illustrate that a broad array of information and assets have been targeted and remain at risk:

- In May 2013, a previously undisclosed section of a confidential report prepared for Pentagon leaders revealed that designs for many of the nation's most sensitive advanced weapons systems had been compromised by Chinese hackers. Plans for the F/A-18 fighter jet, V-22 Osprey, F-22 Raptor fighter jet, Terminal High Altitude Area Defense missile defense system, Littoral Combat Ship, and F-35 Joint Strike Fighter were among those affected.[7]
- In March 2012, it was reported that a security breach at Global Payments, a firm that processed payments for Visa and Mastercard, could compromise the credit and debit-card information of millions of Americans.
- In April 2011, Sony disclosed that it suffered a massive breach in its video game online network that led to the theft of personal information, including the names, addresses, and possibly credit card data belonging to 77 million user accounts.
- On March 17, 2011, RSA, the leading government provider for two-factor authentication devices, disclosed that it had been hacked. Cyber espionage connections have been suggested regarding the theft of other military weapons systems gained during the RSA breach.[8]

The technologies cultivated by Americans are at risk of being stolen by competing nations at the expense of long-term U.S. security. The Office of the National Counterintelligence Executive (ONCIX) states that "the governments of China and Russia will remain aggressive and capable collectors of sensitive US economic information and technologies … in cyberspace."[9] ONCIX also states that "Chinese actors are the world's most active and persistent perpetrators of economic espionage."[10]

The private sector alone lacks the resources and expertise to thwart foreign efforts to steal critical American know-how. This is in large part because counterintelligence is not a typical corporate function, even for well-trained and well–staffed security professionals. These difficulties are also enumerated in the PricewaterhouseCooper's "Global State of Information Security Survey 2013" report, which describes how tight budgets, the rise of mobile devices, and inadequate training for employees have undermined corporations' abilities to effectively address cyber security threats.[11] Whether corporate awareness or expertise is where it needs to be, the

---

[7] *See* "Theft of F-35 design data is helping U.S. adversaries –Pentagon;" *Reuters*; David Alexander; June 19, 2013; http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619.
[8] *See* "Stolen Data Is Tracked to Hacking at Lockheed;" *New York Times*; Christopher Drew; June 3, 2011; http://www.nytimes.com/2011/06/04/technology/04security.html?_r=0.
[9] *Id*. at ii.
[10] *Id*. at i.
[11] *See generally* "*Changing the Game: Key Findings from The Global State of Information Security Survey 2013*;" http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml.

fact remains that the competitive advantage a company has built can be destroyed by the theft of a single piece of intellectual property.

In May 2013, the Commission on the Theft of American Intellectual Property released a report[12] that concluded that the scale of international theft of American intellectual property is unprecedented. The IP Commission estimates that the loss of IP to be roughly $300 billion per year and 2.1 million additional jobs now in our economy. To date, the U.S. response to this new form of espionage is inadequate.[13]

While China is not the only actor targeting U.S. IP and technology, it is the only nation that considers acquiring foreign science and technology a national growth strategy.[14] With unemployment still high, cutting-edge technology is a key to U.S. economic growth. China's broad strategy to target this very technology diminishes this economic growth. Treasury Secretary Lew stated that the administration will continue to stress to China that the theft of IP and technology through cyber espionage "is something that is going to remain high on our agenda of issues to talk with them about."[15]

A. Government Response to U.S. Intellectual Property Theft

The ongoing efforts to steal U.S. companies' IP and other sensitive information are exacerbated by the ever-increasing prevalence and sophistication of cyber-threats facing the nation. While techniques exist to reduce vulnerabilities to cyber-based threats, these require strategic planning by affected entities. Effective coordination among federal agencies responsible for protecting IP and defending against cyber-threats, as well as effective public-private partnerships, are essential elements of any nationwide effort to protect U.S. businesses and economic security.

In the past few years, there has been an increase in enforcement of internet crimes that includes voluntary initiatives by the private sector, improved efficiency and coordination among agencies and progress with trading partners.[16] Criminal enforcement by the Federal Bureau of Investigation, U.S. Immigration and Customs Enforcement and Customs and Border Protection have increased in recent years. Private sector companies have voluntarily agreed to adopt best practices aimed at curbing the sale of counterfeit goods and reducing online piracy. Additionally, the Office of the U.S. Trade Representative is working with partners such as South Korea to negotiate a Trans-Pacific Partnership trade agreement to increase IP protection and enforcement.

---

[12] *See The IP Commission Report*: The Report of the Commission on the Theft of American Intellectual Property (May 2013); http://www.ipcommission.org/Report/index.html.
[13] *See* Transcript of Gov. Jon Huntsman detailing the findings of the IP Commission report; May 22, 2013; http://www.ipcommission.org/Report/IP_Commission_052213_Transcript.pdf.
[14] *See* "China's Twelfth Five Year Plan (2011-2015) – the Full English Version," British Chamber of Commerce in China, 2011; http://www.britishchamber.cn/content/chinas-twelfth-five-year-plan-2011-2015-full-english-version.
[15] *See* "U.S. to press China on cyber theft: Lew:" *Reuters*, July 1, 2013.
[16] *See 2013 Joint Strategic Plan on Intellectual Property Enforcement Report*; http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

In March 2012, Department of Commerce, released an economic report titled *Intellectual Property and the U.S. Economy: Industries in Focus*,[17] detailing the importance of IP and the interconnectivity between IP protection and workforce security. The report concluded that, in 2010 alone:

- IP accounted for $5.06 trillion in value added, or 34.8 percent of U.S. GDP;
- IP created 27.1 million jobs and indirectly supported another 12.9 million jobs
- IP accounted for over 60 percent of all U.S. exports; and
- The average weekly wage in IP industries was 42 percent higher than in other industries.

III. ISSUES

The following issues will be examined at the hearing:

- The scope and nature of the cybersecurity threats to U.S. intellectual property and technology.
- Proposed solutions to better protect U.S. intellectual property and technology from cyber threats, including best practices, enhanced information sharing, and public-private partnerships.
- Policy solutions to protect U.S. intellectual property and technology.
- Private sector perspectives on the role of the private sector in protecting assets and mitigating exposure to cyber threats from state actors.

IV. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Carl Anderson at (202) 225-2927.

[17] *See Intellectual Property and the U.S. Economy: Industries in Focus*; http://www.uspto.gov/news/publications/IP_Report_March_2012.pdf.