AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBER ESPIONAGE AND THE THEFT OF U.S. INTELLECTUAL PROPERTY AND TECHNOLOGY

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JULY 9, 2013

Serial No. 113–67

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE
86–391 WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

RALPH M. HALL, Texas
JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

TIM MURPHY, Pennsylvania
Chairman

MICHAEL C. BURGESS, Texas
Vice Chairman
MARSHA BLACKBURN, Tennessee
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
GREGG HARPER, Mississippi
PETE OLSON, Texas
CORY GARDNER, Colorado
H. MORGAN GRIFFITH, Virginia
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

DIANA DEGETTE, Colorado
Ranking Member
BRUCE L. BRALEY, Iowa
BEN RAY LUJAN, New Mexico
EDWARD J. MARKEY, Massachusetts
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
KATHY CASTOR, Florida
PETER WELCH, Vermont
PAUL TONKO, New York
GENE GREEN, Texas
JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California *(ex officio)*

CONTENTS

	Page
Hon. Tim Murphy, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement	1
Prepared statement	3
Hon. Janice D. Schakowsky, a Representative in Congress from the State of Illinois, opening statement	4
Hon. Fred Upton, a Representative in Congress from the state of Michigan, opening statement	6
Prepared statement	6
Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, prepared statement	8
Hon. Henry A. Waxman, a Representative in Congress from the state of California, opening statement	8

WITNESSES

Slade Gorton, Former U.S. Senator from Washington State, Commission Member, Commission on the Theft of American Intellectual Property	10
Prepared statement	12
Answers to submitted questions	82
Larry M. Wortzel, Ph.D., Commissioner, U.S.-China Economic and Security Review Commission	15
Prepared statement	17
Answers to submitted questions	90
James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies	33
Prepared statement	35
Answers to submitted questions	98
Susan Offutt, Chief Economist, Applied Research and Methods, Government Accountability Office	44
Prepared statement	46
Answers to submitted questions	106

SUBMITTED MATERIAL

Letter of July 9, 2013, from Cyber Secure America Coalition to the subcommittee, submitted by Mr. Murphy	76
Letter of July 9, 2013, from Cyber Secure America Coalition to the subcommittee, submitted by Ms. DeGette	79

CYBER ESPIONAGE AND THE THEFT OF U.S. INTELLECTUAL PROPERTY AND TECHNOLOGY

TUESDAY, JULY 9, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:15 a.m., in room 2123, Rayburn House Office Building, Hon. Tim Murphy (chairman of the subcommittee) presiding.

Present: Representatives Murphy, Burgess, Blackburn, Scalise, Olson, Gardner, Johnson, Long, Ellmers, Upton (ex officio), Braley, Schakowsky, Tonko, Green, and Waxman (ex officio).

Staff Present: Carl Anderson, Counsel, Oversight; Sean Bonyun, Communications Director; Matt Bravo, Professional Staff Member; Megan Capiak, Staff Assistant; Karen Christian, Chief Counsel, Oversight; Patrick Currier, Counsel, Energy & Power; Andy Duberstein, Deputy Press Secretary; Brad Grantz, Policy Coordinator, O&I; Sydne Harwick, Staff Assistant; Brittany Havens, Staff Assistant; Sean Hayes, Counsel, O&I; Andrew Powaleny, Deputy Press Secretary; Peter Spencer, Professional Staff Member, Oversight; Brian Cohen, Minority Staff Director, Oversight & Investigations, Senior Policy Advisor; Kiren Gopal, Minority Counsel; and Hannah Green, Minority Staff Assistant.

OPENING STATEMENT OF HON. TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. MURPHY. Good morning. I convene this hearing of the Subcommittee on Oversight and Investigations entitled "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology. In the last several months, there have been increasing reports of cyber espionage and its toll on U.S. businesses and the economy. In March, Thomas Donilon, the National Security Advisor to the President, addressed the issue of cyber espionage and the theft of U.S. Intellectual property, or IP, and technology, particularly in China. Mr. Donilon stated that IP and trade secrets "have moved to the forefront of our agenda. Targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China occurs on an unprecedented scale. The international community cannot afford to tolerate such activity from any country."

In June, President Obama raised this issue with the Chinese president during a summit in California, and I thank him for pushing this issue so critically important to U.S. jobs. Just 2 weeks ago, the Council on Foreign Relations released a report finding that U.S. oil and natural gas operations are increasingly vulnerable to cyber attacks and that these attacks damage the competitiveness of these companies. The victims go beyond the energy industry, though. A recent report by a cyber security consulting firm documented the Chinese People Liberation Army's direct involvement with cyber attacks and espionage into 141 companies, including 115 in the U.S. across 20 industries.

Three years ago, Chinese military hackers infiltrated the Pittsburgh location of QinetiQ, a manufacturer of high tech robotic systems, like the remotely-controlled devices used to diffuse IEDs. Experts believe the Chinese hackers may have stolen from QinetiQ's proprietary chip architecture, allowing the PLA to take over or defeat U.S. military robots and aerial drones. From defense contractors to manufacturers, no American company has been immune from the scourge of Chinese intellectual property theft.

In January, two Chinese citizens were convicted for attempting to steal trade secrets from a Pittsburgh Corning plant in order to build a rival factory in China. Cyber espionage has obvious implications for national security, foreign relations, and the American economy.

The IP Commission, which Senator Slade Gorton represents today, recently published a report on the theft of intellectual property and estimated that it costs the U.S. economy over $300 billion a year, which translates roughly to 2.1 million lost jobs. To put this in perspective, the IP Commission found that the total cost of cyber theft was comparable to the amount of U.S. exports to Asia. General Keith Alexander, the director of the National Security Agency called cyber crime and the resulting loss of our intellectual property and technology to our competitors "the greatest transfer of wealth in U.S. history."

The purpose of this hearing is to understand how this loss is happening, the cost to our country, and how companies and the U.S. government are responding to this threat. The testimony of the IP Commission and the U.S.-China Commission make clear that the People's Republic of China is the most predominant and active source of cyber espionage and attacks. China, while the main source, is not the only one. The Office of the National Counter Intelligence Executive states Russia, too, is aggressively pursuing U.S. IP and technology.

The witnesses today will explain the methods and tactics used to penetrate U.S. cyber systems and what China and other perpetrators do with the information they obtain through these attacks. Counterfeiting of U.S. products and technologies is often an unfortunate result of cyber espionage attacks. In an op-ed submitted to the Washington Post, Admiral Dennis Blair, former Director of National Intelligence, and Jon Huntsman, Jr., the former Ambassador to China, explain how the counterfeiting of a U.S. product by a foreign company resulted in the foreign company's becoming the largest competitor to that U.S. company.

Ultimately, the U.S. company's share price fell 90 percent in just 6 months. Just last month, Federal prosecutors secured an indictment against Sinovel, a Chinese wind turbine company, for stealing source code for small industrial computers used in wind turbines for a U.S. business, American Semiconductor Company. The CEO of American Semiconductor remarked on the reported $1 billion loss in market value his company suffered as a result of this theft, stating "If your ideas can be stolen without recourse, there is no reason to invest in innovation. There is no purpose to the American economy."

So I'd like to thank the witnesses today. First, we have the Honorable Slade Gorton, the former Senator from the State of Washington, and currently a Commission member of the Commission on the Theft of American Intelligence Property. Joining him is an expert on cyber security and Chinese foreign policy, the Honorable Larry Wortzel, Ph.D., who is a Commissioner on the U.S.-China Economic and Security Review Commission; Dr. James Lewis, Ph.D., a Senior Fellow and Director of the Technology and Public Policy Program at the Center for Strategic International Studies; and Susan Offutt, Chief Economist for the Applied Research and Methods with the General Accountability Office.

We invited a spokesman from the White House and the administration to join us today, but they informed the committee that they would respectfully decline its invitation. It is unfortunate that the administration wasn't able to take this opportunity to join us and testify, given the importance of this issue and the priority the administration has given it during recent talks with the Chinese president. That invitation remains open for them to meet with us.

So with that, I recognize the ranking member, Ms. Schakowsky, who is now sitting in for—by designation for Ms. DeGette. You are recognized for 5 minutes.

[The prepared statement of Mr. Murphy follows:]

PREPARED STATEMENT OF HON. TIM MURPHY

In the last several months, there have been increasing reports of cyber espionage and its toll on U.S. businesses and the economy. In March, Thomas Donilon, the National Security Advisor to the President, addressed the issue of cyber espionage and the theft of U.S. intellectual property, or "IP," and technology, particularly by China. Mr. Donilon stated that IP and trade secrets "have moved to the forefront of our agenda...targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China [occurs] on an unprecedented scale. The international community cannot afford to tolerate such activity from any country." In June, President Obama raised this issue with the Chinese President during a summit in California.

Just 2 weeks ago, the Council on Foreign Relations released a report finding that U.S. oil and natural gas operations are increasingly vulnerable to cyber attacks, and that these attacks damage the competitiveness of these companies. The victims go beyond the energy industry, though. A recent report by a cybersecurity consulting firm documented the Chinese People Liberation Army's direct involvement through cyber attacks and espionage into 141 companies, including 115 in the U.S., across 20 industries.

Three years ago, Chinese military hackers infiltrated the Pittsburgh location of QinetiQ, a manufacturer of high-tech robotic systems like the remotely-controlled devices used to diffuse IEDs. Experts believe the Chinese hackers may have stolen from QinetiQ's proprietary chip architecture, allowing the PLA to take over or defeat U.S. military robots and aerial drones.

From defense contractors to manufacturers, no American company has been immune from the scourge of Chinese intellectual property theft. In January, two Chi-

nese citizens were convicted for attempting to steal trade secrets from a Pittsburgh Corning plant in order to build a rival factory in China.

Cyber espionage has obvious implications for national security, foreign relations, and the American economy. The Commission, which Senator Slade Gorton represents today, recently published a report on the theft of intellectual property and estimated that it costs the U.S. economy over $300 billion a year, which translates into roughly 2.1 million lost jobs. To put this in perspective, the IP Commission found that the total cost of cyber theft was comparable to the amount of U.S. exports to Asia. General Keith Alexander, the director of the National Security Agency, called cyber crime, and the resulting loss of our intellectual property and technology to our competitors, "the greatest transfer of wealth in history."

The purpose of this hearing is to understand how this loss is happening, the cost to our country, and how companies and the U.S. government are responding to this threat. The testimony of the IP Commission and the U.S.-China Commission make clear that the People's Republic of China is the most predominant and active source of cyber espionage and attacks. China, while the main source, is not the only one. The Office of the National Counterintelligence Executive (ONCIX) states Russia, too, is aggressively pursuing U.S. IP and technology.

The witnesses today will explain the methods and tactics used to penetrate U.S. cyber systems, and what China and other perpetrators do with the information they obtain through these attacks. Counterfeiting of U.S. products and technologies is often an unfortunate result of cyber espionage attacks. In an op-ed submitted to the Washington Post, Admiral Dennis Blair, former director of national intelligence, and Jon Huntsman, Jr., the former ambassador to China, explained how the counterfeiting of a U.S. product by a foreign company resulted in the foreign company becoming the largest competitor to that U.S. company. Ultimately, the U.S. company's share price fell 90 percent in just 6 months.

Just last month, federal prosecutors secured an indictment against Sinovel, a Chinese windturbine company, for stealing source code for small industrial computers used in wind-turbines for a U.S. business, American Semiconductor Company. The CEO of American Semiconductor remarked on the reported $1 billion loss in market value his company suffered as a result of this theft, stating, "...If your ideas can be stolen without recourse, there is no reason to invest in innovation, there is no purpose to the American economy."

I would like to thank the witnesses. First, we have the Honorable Slade Gorton the former Senator from the State of Washington and currently a Commission Member on the Commission on the Theft of American Intellectual Property. Joining him is an expert on cyber security and Chinese foreign policy, the Honorable Larry M. Wortzel, Ph.D., who is a Commissioner on the U.S.-China Economic and Security Review Commission; Dr. James Lewis, Ph.D. a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS); and Susan Offutt, Chief Economist for Applied Research and Methods with the General Accountability Office.

We invited a spokesperson from the White House and the administration to join us today, but they informed the committee that they would respectfully decline its invitation. It is unfortunate that the administration did not take this opportunity to join us and testify given the importance of this issue and the priority the administration has given it during its recent talks with the Chinese President.

# # #

OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. Before I begin, let me give a special welcome to Senator Gorton, who I understand grew up in my hometown of Evanston, Illinois, which I now have the pleasure of representing, and to welcome you and all the other witnesses here today.

The President, in his State of the Union address this year, said "Our enemies are seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems." And the President's right. And that is why I am so glad that we're hav-

ing today's hearing to learn about the impact of cyber espionage, the theft of intellectual property, and the threat that they pose to our economy and national security.

The GAO has indicated that "The theft of U.S. intellectual property is growing and is heightened by the rise of digital technologies." The Obama Administration has taken a leading role in the effort to root out cyber threats. The President's cyberspace policy review identified and completed 10 near-term actions supporting our Nation's cyber security strategy. The Department of Homeland Security has created a cyber security incident response plan; the National Institute of Standards and Technology in 7 months is expected to publish voluntary standards for operators of our Nation's critical infrastructure that will help mitigate the risks of cyber attacks.

The private sector has also taken steps independently to root out cyber threats and increased communication about best practices for combating malicious attacks. Those public and private sector efforts have strengthened Americans' defenses and protected our critical infrastructure and intellectual property. We know that foreign actors are seeking access to American military intelligence and corporate trade secrets. China, Russia, and other countries continue to deploy significant resources to gain sensitive proprietary information via cyber attacks.

While I strongly believe we need to address cyber security concerns, I did vote against the Cyber Intelligence Sharing and Protection Act. I believe the bill, though improved from the last Congress, does an inadequate job of defending the privacy rights of ordinary Americans. We can't compromise our civil liberties in exchange for a strong defense against cyber attacks. We need a better balance, and I'm committed to working toward that end. We will hear today from Larry Wortzel——

Am I saying that right?

Mr. WORTZEL. Yes.

Ms. SCHAKOWSKY. A member of the U.S.-China Economic and Security Review Commission, that China is. And I quote, "Using its advanced cyber capabilities to conduct large-scale cyber espionage, and China has compromised a range of U.S. networks, including those at the Department of Defense, defense contractors, and private enterprises."

Mr. Wortzel's testimony provides examples of those intrusions, thousands of targeted attacks on DOD network, a case where hackers gained full functional control—that's a quote—over the NASA Jet Propulsion Lab network, and Chinese cyber attacks on the major contractors for the F–35 joint strike fighters. It describes a U.S. super computer company that was devastated when its high-tech secrets were stolen by a Chinese—a Chinese company, and it highlights the Night Dragon operation, where multiple oil, energy, and petrochemical companies were targeted for cyber attacks, that gave outside hackers access to executive accounts and highly sensitive documents for several years.

Mr. Chairman, we cannot take these problems lightly. I know you don't. They cost our economy billions of dollars and places our national security at risk. And as the number of Internet-connected devices and the use of cloud computing increases, the number of

entry points for malicious actors to exploit will also rise. With more information and more sensitive information now stored on the Web, we must sharpen our focus on cyber security. I hope to hear more from our witnesses today about this immense challenge and how the private sector and government entities can become more cyber resilient. And with that, I yield back, Mr. Chairman.

Mr. MURPHY. Gentlelady yields back. Now to the chairman of the full committee, Mr. Upton, for 5 minutes.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. Well, thank you, Mr. Chairman. Today's hearing continues the Energy and Commerce Committee's oversight of cyber threats and cybersecurity. This committee has jurisdiction over a number of industries and sectors that have long been the target of cyber attacks and espionage, including the oil and gas industry, the electric utility industries, the food services and pharmaceuticals industries, information technology, telecommunications, and high-tech manufacturing. Just last May, Vice Chair Blackburn convened a full committee hearing to examine the mounting cyber threats to critical infrastructure and efforts to protect against them.

Today we're going to focus on the damaging cost to U.S. industry when the efforts of foreign nations and hackers to steal U.S. technology and intellectual property are successful. American innovation and intellectual property are the foundations of our economy. Based on government estimates from 2010, intellectual property accounted for $5 trillion in value, added to the U.S. economy are 34 percent of U.S. GDP. When foreign nations are able to infiltrate networks and take our technology and proprietary business information to benefit their own companies, U.S. firms certainly lose their competitive advantage. The IP Commission, on whose behalf we welcome former Senator Slade Gorton's testimony this morning, has translated the cost of these attacks into hard numbers.

As Chairman Murphy mentioned, this theft costs the U.S. over 300 billion a year, over 2 million jobs that are lost. And if our IP is being targeted, U.S. Jobs are being targeted, and this has got to stop. I'm especially interested in learning more from today's witnesses about the growing threat, how the U.S. Government is combating it, and what American job creators themselves can do to protect against the theft of their intellectual property. We're going to continue our efforts to protect our nation from the ever-growing cyber threat. It is an issue that commands and demands our immediate attention. And I yield the balance of my time to Ms. Blackburn.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON

Today's hearing continues the Energy & Commerce Committee's oversight of cyber threats and cyber security. This committee has jurisdiction over a number of industries and sectors that have long been the target of cyber attacks and espionage, including the oil and gas industry, the electric utility industries, the food services and pharmaceuticals industries, information technology and telecommunications, and hightech manufacturing. Just last May, Vice Chairman Blackburn convened a full committee hearing to examine the mounting cyber threats to critical infrastructure and efforts to protect against them.

Today, we focus on the damage and costs to U.S. industry when the efforts of foreign nations and hackers to steal U.S. technology and intellectual property are successful. American innovation and intellectual property are the foundations of our economy. Based on government estimates from 2010, intellectual property accounted for $5.06 trillion in value added to the U.S. economy or 34.8 percent of U.S. GDP. When foreign nations are able to infiltrate networks and take our technology and proprietary business information to benefit their own companies, U.S. firms lose their competitive advantage. The IP Commission, on whose behalf we welcome former Senator Slade Gorton's testimony this morning, has translated the costs of these attacks into hard numbers: as Chairman Murphy mentioned, this theft costs the United States over $300 billion a year, and 2.1 million lost jobs. If our IP is being targeted, U.S. jobs are being targeted, and this must stop.

I am especially interested in learning more from today's witnesses about this growing threat; how the U.S. government is combatting it; and what American job creators themselves can do to protect against the theft of their intellectual property.

We will continue our efforts to protect our nation from the ever-growing cyber threat. It is an issue that commands and demands our immediate attention.

# # #

Mrs. BLACKBURN. I thank the chairman. I welcome each of you. And as you can hear from the opening statements, we all agree that every single employer in this country has the potential of being harmed by cyber attacks. We realize that and we know it is a problem that has to be addressed. And I thank Chairman Murphy for calling the hearing today. Cyber espionage, hacking, stealing trade secrets is an escalating activity, and we need to put an end to this. I also believe that in addressing our cyber security challenges, we need to expand the scope of our efforts to address the related issue of IP theft. As both Chairman Murphy and Upton have said, it is over $300 billion a year in what it costs our economy. And this is a cost that becomes more expensive for us every year as the problem grows.

Countries like China and Russia are engaging in wholesale commercial espionage. They are intentionally taking advantage of U.S. technology and creativity for their own competitive advantages. It is an economic growth strategy for them, but it's a jobs killer, a national security threat, and a privacy nightmare for Americans. I've offered a discussion framework, the Secure IT Act, that provides our Government, business community, and citizens with the tools and resources needed to protect us from those who wish us harm. It would help us respond to those who want to steal our private information, it better protects us from threats to both our Government systems and to the private sector without imposing heavy-handed regulations that would fail to solve these persistent, dynamic, and constantly evolving changes that we are facing. With that, I yield the balance of my time to Dr. Burgess.

Mr. BURGESS. I thank the gentlewoman for yielding. I'll submit my full statement to the record. I do want to address an issue that may be a little bit outside the purview of the panelists today. But, Mr. Chairman, I do hope we'll devote some time to this at some point. Individuals, of course, have limited liability; if our credit card numbers are stolen by a bad actor or a criminal, there is a limit to the amount that that fraudulent transfer can be. But that's not true for our small businesses in this country. And I'm thinking particularly of the doctor's office, the dentist's office, the CPA, the small law firm who may have their—in fact, in health care, we're

required now to do electronic transfers for Medicare and for other activities. There is no limit of liability to those small practices. If their information is hacked and stolen, no, it's not going to be by on sovereign nation, it's going to be by a criminal. But, nevertheless, they are hacked and the information is stolen. Sensitive patient data or customer data then is retrieved by the bad actor.

I hope we will address at some point the ability to limit the liability of those small practices when, in fact, they are only doing what they have been required to do by the Federal Government and the Medicare system.

Thank you, Mr. Chairman. I'll yield back the balance of the time.

[The prepared statement of Mr. Burgess follows:]

PREPARED STATEMENT OF HON. MICHAEL C. BURGESS

Thank you, Mr. Chairman.

One of the largest threats facing our nation today is that of cyber-security and espionage from a variety of sources. Indeed, top national security advisors have recently stated that cyber-security was the number one danger to the United States - even going so far as to supplant terrorism as a greater threat.

The constant threat of cyber-security and espionage target not just our nation's defenses, but also sensitive personal and proprietary information. All kinds of American businesses are targeted for their trade secrets, business plans and sensitive data. And, unfortunately, many times, the bad actors are successful.

This is a stark contrast from before where our state secrets were only being targeted. Experts' estimate that the annual private sector loss from cyber-attacks to be in the tens of billions of dollars. In fact, NSA Director Gen. Keith Alexander has stated that the stealing of U.S. private company information and technology has resulted in the ″greatest transfer of wealth in history.″ To make matters worse, these cyber-attacks seem to be only growing in number and many predict that the intensity and number of attacks will increase significantly throughout the coming years.

The importance of intellectual property in the U.S. economy cannot be overstated. In 2010, IP accounted for $5 trillion in value or 34% of U.S. GDP. IP also has accounted for over 60% of all US exports and independently created tens of millions of jobs. Needless to say, the interconnectivity between IP protection and workforce security is paramount.

This hearing could not come at a more appropriate time. Yesterday marked the first meeting of a U.S.-China cyber-security working group. This is an important first step to enable each side to share perspectives on pertinent laws and norms in cyberspace. I hope that the outcome of this hearing, as well as those discussions, will be to shed light on a growing threat because the unwarranted and unprovoked theft of U.S. private and public intellectual property has to stop.

Thank you, Mr. Chairman and I yield back.

Mr. MURPHY. Gentleman yields back. Mr. Waxman recognized for 5 minutes.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you very much, Mr. Chairman. I am pleased that we're here today to discuss the problem of cyber espionage and theft of U.S. intellectual property. Cyber espionage damages our economy and places national security at risk. The threats posed by cyber espionage are growing, particularly from foreign actors. Numerous reports have noted that the Chinese government is the chief sponsor of hacking activity directed at sensitive military information and lucrative corporate trade secrets. The Department of Defense reported that in 2012, computer systems including those owned by the U.S. Government were targeted directly thousands of

times by the Chinese government and military. The New York Times reported that more than 50 sensitive U.S. technologies and advanced weapons systems, including the Patriot Missile System, had been compromised by Chinese hackers.

The computer security consultant Mandiant reported over a hundred instances of network intrusions affecting key industries and industry leaders located in the United States originating from one building in Shanghai. Even an iconic American company, Coca-Cola, had key corporate documents exposed by Chinese hackers, compromising a multi-billion dollar acquisition. Thankfully, they did not get the formula. My ad lib.

The White House recognizes the seriousness of the threat and has been leading the response. Over the past 3 years, law enforcement has significantly increased against infringement that threatens our economy. Trade secret cases are up, DHS seizures of infringing imports have increased, and FBI health-and-safety-focused investigations are up over 300 percent. And in February, President Obama signed an executive order to strengthen the cyber security of our critical infrastructure and direct DHS to share threat information with U.S. businesses. And just last month, the administration released a new strategic plan for intellectual property enforcement. But the administration needs Congress's help, and we are not delivering. Earlier this year, the House passed a Cyber Intelligence and Sharing Protection Act. This is a flawed bill that relies on a purely voluntary approach. It sets no mandatory standards for industry, yet it would give companies that share information with the government sweeping liability protection. The legislation also fails to safeguard the personal information of Internet users.

The bill is now pending in the Senate. I hope the Senate comes up with an acceptable compromise. I want to pass a law that improves our ability to prevent cyber attacks while adequately protecting the privacy of individuals' data. Cyber attacks jeopardize our economic and national security, they threaten key defense technologies, they can impact basic infrastructure like our power grid and traffic control systems, and they can endanger innovation by America's leading corporations. That's why we must have a comprehensive and nimble strategy to mitigate against risks of cyber attacks. The White House, the private sector, and Congress must each do its part.

I look forward to hearing from our witnesses today about what more we can do to address the serious threats posed by cyber espionage. Thank you, Mr. Chairman. Yield back the balance of my time.

Mr. MURPHY. Gentleman yields back. Thank you.

And I already introduced the witnesses, so I don't need to go through those again, but we thank them all for being here. To the witnesses, you are aware that the committee is holding an investigative hearing. When doing so, has a practice of taking testimony under oath. Do you—any of you have any concerns or objections to testifying under oath?

No. None, OK. Thank you.

The chair, then, advises you that under the rules of House and the rules of committee, you are entitled to be advised by counsel.

Do any of you desire to be advised by counsel during the testimony today?

All the witnesses indicate no.

In that case, if you'd all please rise, raise your right hand, I'll swear you in.

[Witnesses sworn.]

Mr. MURPHY. Thank you. All the witnesses indicated that they do.

So you are now under oath and subject to the penalties set forth in Title 18, Section 1001 of the United States Code.

You may now each give a 5-minute summary of your written statement. We'll start with you, Senator Gorton. Welcome here. You are recognized for 5 minutes.

STATEMENTS OF HON. SLADE GORTON, FORMER U.S. SENATOR FROM WASHINGTON STATE, COMMISSION MEMBER, COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY; LARRY M. WORTZEL, PH.D., COMMISSIONER, U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION; JAMES A. LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES; AND SUSAN OFFUTT, CHIEF ECONOMIST, APPLIED RESEARCH AND METHODS, GOVERNMENT ACCOUNTABILITY OFFICE

STATEMENT OF HON. SLADE GORTON

Mr. GORTON. Mr. Chairman, Madam——

Mr. MURPHY. Pull it close to you. These microphones in the House are not as good as Senate ones.

Mr. GORTON [continuing]. Representative of the city in which I grew up, I thank you for your greetings. I was a member of the Intellectual Property Theft Commission, headed by former Governor Jon Huntsman and former Admiral Dennis—Dennis Blair, President Obama's first Director of National Intelligence. It had three goals. The first was to chart the dimensions of the intellectual property theft and their impact on the United States.

Second, to separate the rather large part of that that comes from the People's Republic of China. And, third, to make recommendations to the administration and to the Congress about what—what to do about it. Two of you have already pointed out that we found a minimum of $300 million a year of losses to the American economy through intellectual property theft, representing a couple of million jobs. Just imagine what that would do for us all by itself, without any of the debates which have rocked—rocked this Congress.

I would say at the beginning that it isn't just cyber enterprise, cyber theft. Cyber theft is a major part of stealing trade secrets, but there's also a violation of copyright and trademark protections and patent infringement. For example, one software developer in the United States reported to us that a few years ago, it sold one software program in China for approximately $100. A year later, when there was an automatic update available, it had 30 million calls from China. 30 million to 1. That wasn't cyber enterprise, that was just reverse engineering a piece of software.

Now, China accounts for 50 to 80 percent of this intellectual property loss. Much of which, maybe even most of which is from private sector Chinese firms. But they are able to do that because the sanctions in China for violations, even when they are caught, are extremely small and rarely enforced.

Now, what that leads me to say is that while we—that every one of the recommendations that we have made in this commission report will help, they are primarily defensive in nature. And it is clear that we need better defensive measures to deal with cyber theft and other forms of intellectual property theft. But I am convinced that that will never solve the problem on its own. What we need to do is to come up with policy responses that create interest groups in China and in the other violators that value intellectual property protection. When there is a major interest group in China that says this is hurting us rather than helping us, we will have begun to solve the problem. That's a very difficult challenge. A few of the recommendations we make would make steps, appropriate steps in that direction and we recommend them to you. But think from the very beginning, how do we create an interest group that is on our side in the countries that are engaged in this kind of theft.

Our recommendations, including targeting for financial factions, quick response measures for seizing intellectual property-infringing goods at the border when they arrive, and increasing support for the FBI, among others. Finally,I would say that at the very end, in the last 2 pages of our report, we list three other methods of dealing with this matter that aren't our formal recommendations. They are all relatively nuclear in nature. But we commend them to your very, very careful study, each—because each of those carries with it the ability to create that internal group in China itself that will be on—will be on our side.

And with that, I'm at your disposal. The National Bureau of Asian Research, which conducted this, is at your disposal. We want to help you as much as we possibly can. We are convinced that this is not a partisan issue by any stretch of the imagination. And that this committee should be able to come up with unanimous responses that will be of real impact.

Mr. MURPHY. Thank you, Senator.

[The prepared statement of Mr. Gorton follows:]

THE

IP COMMISSION

THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY

July 9, 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 House Energy & Commerce Committee;
Subcommittee on Oversight and Investigations

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 creates 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, patent infringement, and stealing trade secrets. Trade secrets are stolen through cyber espionage, traditional means of industrial and economic espionage, or frequently a combination of both. Admiral Blair makes the point that in most successful cases in which cyber is used to steal IP, it is used in combination with bribed or planted disloyal employees, stealing documents, physically breaking into computers, wire-tapping, bugging, or other time-tested methods.

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 much of the public discourse surrounding the issue focuses on hacking and cyber-theft, 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. While it is true that the rise of personal computing has added a new dynamic to protecting intellectual property, however, 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 New York University 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 you 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 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.

Along with my testimony today, I am submitting a copy of the IP Commission's report that was released on May 22, 2013. The final chapters lay out a series of policy recommendations, organized as short, medium, and long-term recommendations. 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, quick response measures for seizing IP infringing goods at the border, and increasing FBI resources to more aggressively pursue criminal cases against IP violators. 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 recommendations specifically relating to the cyber dimensions of IP theft.

The recommendations vary by subject matter and would likely fall under the jurisdiction of a number of different Congressional committees. Especially relevant to this committee is our recommendation to establish the Secretary of Commerce as the principal government official responsible for enhancing and implementing policies regarding the protection of intellectual property, enforcement of implementation actions, and policy development. The Secretary of Commerce has sufficient human, budget, and investigative resources to address the full range of IP-protection issues. The Under Secretary of Commerce for Intellectual Property & Director of the U.S. Patents and Trademarks Office is already the president's advisor on intellectual property policy. In addition, much of the executive authority for many of our other recommendations,

such as the quick response seizures at the border and the targeted financial sanctions, we recommend be vested in the Secretary of Commerce.

We hope that this report and its recommendations will help to inform and strengthen the policy changes that must come from Congress and the Administration to be effective.
Thank you.

Mr. MURPHY. Dr. Wortzel, you are recognized for 5 minutes. Please bring the microphone real close to your mouth so we can hear. Thank you.

STATEMENT OF LARRY M. WORTZEL

Mr. WORTZEL. Chairman Murphy, Ranking Member Schakowsky, members of the subcommittee. I'll discuss the role of China's government, its military and intelligence services, and its industries and cyber espionage and the theft of U.S. intellectual property. My testimony presents some of the U.S.-China Economic and Security Review Commission's findings on China's cyber espionage efforts, but the views I present today are my own. In 2005, Time Magazine documented the penetration of Department of Energy facilities by China in the Titan Rain intrusion set. So this cyber espionage has been going on for quite some time. China's using its advanced cyber capabilities to conduct large-scale cyber espionage, and has, to date, compromised a range of U.S. networks, including those of the Department of Defense—Departments of Defense, State, Commerce, and Energy, defense contractors, and private enterprises.

China's cyber espionage against the U.S. Government and our defense industrial base poses a major threat to U.S. military operations, the security of U.S. military personnel, our critical infrastructure, and U.S. industries. China uses these intrusions to fill gaps in its own research programs, to map future targets, to gather intelligence on U.S. Strategies and plans, to enable future military operations, to shorten research and development timelines for new technologies, and to identify vulnerabilities in U.S. systems.

In my view, it's helpful when government and industry expose the intrusions and make the public aware of them. Businesses unfortunately are reluctant to do so. China's cyber espionage against U.S. commercial firms poses a significant threat to U.S. business interests and competitiveness.

General Keith Alexander, Director of the National Security Agency, assessed that the value of these losses is about $338 billion a year, although not all the losses are from China. That's the equivalent of the cost of 27 Gerald R. Ford class aircraft carriers. The Chinese government, military, and intelligence agencies support these activities by providing state-owned enterprises information extracted through cyber espionage to improve their competitiveness, cut R&D timetables, and reduces costs. The strong correlation between compromised U.S. companies and those industries designated by Beijing as strategic further indicate state sponsorship, direction, and execution of China's cyber espionage.

Such governmental support for Chinese companies enables them to out-compete U.S. companies, which do not have the advantage of levering government intelligence data for commercial gain. It also undermines confidence in the reliability of U.S. brands. There's an urgent need for Washington to compel Beijing to change its approach to cyberspace and deter future Chinese cyber theft. My personal view is that the President already has an effective tool in the International Emergency Economic Power Enhancement Act. He could declare that this massive cyber theft of intellectual prop-

erty represents an extraordinary threat to the national security, foreign policy, and economy of the United States.

Under that declaration, the President, in consultation with Congress, may investigate, regulate, and freeze transactions and access as well as block imports and exports in order to address the threat of cyber theft and espionage. The authority has traditionally been used to combat terrorist organizations and weapons proliferation, but there's no statutory prohibition or limitation that prevents the President from applying it to cyber espionage issues. If some version of Senate Bill 884 becomes law, it should be expanded to direct the State Department to work with and encourage allied countries to develop similar laws. I want to thank you for the opportunity to appear today, and I'm happy to respond to any questions you may have.

Mr. MURPHY. Thank the gentleman.

[The prepared statement of Mr. Wortzel follows:]

"Cyber Espionage and the Theft of U.S. Intellectual Property and Technology"
Testimony of Larry M. Wortzel
before the House of Representatives
Committee on Energy and Commerce Subcommittee on Oversight and Investigations
July 9, 2013
SUMMARY OF TESTIMONY

I will discuss the role of the People's Republic of China, its military and intelligence services, and its industries in cyber espionage and the theft of U.S. intellectual property and technology. As a member of the U.S.-China Economic and Security Review Commission, I will present some of the Commission's findings on China's cyber espionage efforts, its policies and its goals in stealing technology and intellectual property. The views I present today, however, are my own.

China is using its advanced cyber capabilities to conduct large-scale cyber espionage. China to date has compromised a range of U.S. networks, including those of the Department of Defense (DOD), defense contractors, and private enterprises. These activities are designed to achieve a number of broad security, political, and economic objectives.

China's cyber espionage against the U.S. government and defense industrial bases poses a major threat to U.S. military operations, the security and well-being of U.S. military personnel, the effectiveness of equipment, and readiness. China apparently uses these intrusions to fill gaps in its own research programs, map future targets, gather intelligence on U.S. strategies and plans, enable future military operations, shorten research and development (R&D) timelines for military technologies, and identify vulnerabilities in U.S. systems and develop countermeasures.[1]

China's cyber espionage against U.S. commercial firms poses a significant threat to U.S. business interests and competiveness in key industries. General Keith Alexander, Director of the National Security Agency and commander of U.S. Cyber Command, assessed that the financial value of these losses is about $338 billion a year, including intellectual property losses and the down-time to respond to penetrations, although not all those losses are to Chinese activity.[2] Chinese entities engaging in cyber and other forms of economic espionage likely conclude that stealing intellectual property and proprietary information is much more cost-effective than investing in lengthy R&D programs.[3] These thefts support national science and technology development plans that are centrally managed and directed by the PRC government.

---

[1] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 166.
[2] Josh Rogin, "NSA Chief: Cybercrime Consitutues the 'Greatest Transfer of Wealth in History'," *Foreign Policy: The Cable,* July 9, 2012, *http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history*
[3] Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery is a National Policy – And Must Be Challenged," *Wall Street Journal,* January 27, 2012. *http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html.*

The Chinese government, including the PLA and the Ministry of State Security, supports these activities by providing state-owned enterprises (SOEs) information and data extracted through cyber espionage to improve their competitive edge, cut R&D timetables, and reduce costs. The strong correlation between compromised U.S. companies and those industries designated by Beijing as "strategic" industries[4] further indicates a degree of state sponsorship, and likely even support, direction, and execution of Chinese economic espionage.[5] Such governmental support for Chinese companies enables them to out-compete U.S. companies, which do not have the advantage of leveraging government intelligence data for commercial gain.[6]

There is an urgent need for Washington to compel Beijing to change its approach to cyberspace and deter future Chinese cyber theft. The Chinese government does not appear to be inclined to curb its cyber espionage in any substantial way. Merely naming will not affect this centrally directed behavior.

---

[4] The Commission on the Theft of Intellectual Property, *The IP Commission Report*, (Washington, DC: National Bureau of Asian Research, May 2013), p. 12. *http://ipcommission.org/report/IP_Commission_Report_052213.pdf.*

[5] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 156.

[6] In the late 1980s and early 90s a debate took place in Congress on whether the U.S. Intelligence Community (IC) should share information and/or intelligence assets with U.S. companies to provide those companies an advantage against foreign competitors. In 1991, Director of the Central Intelligence Agency Robert Gates, in a speech to the IC, stated clearly that the CIA would limit itself to helping U.S. companies safeguard themselves from foreign intelligence operations. Robert Gates, "The Future of American Intelligence," (Washington, DC: U.S. Intelligence Community, December 4, 2011).

"Cyber Espionage and the Theft of U.S. Intellectual Property and Technology"

Testimony of Larry M. Wortzel

before the House of Representatives

Committee on Energy and Commerce Subcommittee on Oversight and Investigations

July 9, 2013

Chairman Murphy, Ranking Member DeGette, members of the Subcommittee, thank you for the opportunity to testify today. I will discuss the role of the People's Republic of China, its military and intelligence services, and its industries in cyber espionage and the theft of U.S. intellectual property and technology. As a member of the U.S.-China Economic and Security Review Commission, I will present some of the Commission's findings on China's cyber espionage efforts, its policies and its goals in stealing technology and intellectual property. The views I present today, however, are my own.

China's cyber espionage activities have been going on for a long time. In 2005, *Time* magazine documented a series of intrusions into U.S. laboratories, including those of the Department of Energy, that was called the *Titan Rain* intrusion set.[1] Corporations often will not disclose cyber penetrations and intellectual property theft because they fear retaliation from the Chinese government, hope for future market access in China, fear the loss of consumer confidence, and fear the loss of stock value.

[1] Nathan Thornborough, "The Invasion of the Chinese Cyberspies (and the man who tried to stop them): An Exclusive Look at how the Hackers called TITAN RAIN are Stealing U.S. Secrets," *Time Magazine*, September 5, 2005 *http://www.cs.washington.edu/education/courses/csep590/05au/readings/titan.rain.htm.*

In Chinese military writings, cyberspace is an increasingly important component of China's comprehensive national power, and a critical element of its strategic competition with the United States.[2] Beijing seems to recognize that the United States' current advantages in cyberspace allow Washington to collect intelligence, exercise command and control of military forces, and support military operations. At the same time, China's leaders fear that the United States may use the open Internet and cyber operations to threaten the Chinese Communist Party's (CCP) legitimacy.

China is using its advanced cyber capabilities to conduct large-scale cyber espionage. To date, China has compromised a range of U.S. networks, including those of the Department of Defense (DOD), defense contractors, and private enterprises. These activities are designed to achieve a number of broad security, political, and economic objectives.

China does not appear to have reduced its cyber effort against the United States despite recent public exposure of Chinese cyber espionage in technical detail.[3] When confronted with public accusations from the United States about its cyber espionage, Beijing usually attempts to refute evidence by pointing to the anonymity of cyberspace and the lack of verifiable technical forensic data. It also shifts the media focus by portraying itself as the victim of Washington's cyber activities and calling for greater international cooperation on cyber security.[4] For example, in response to DOD's 2013 report to Congress, which indicated that China participates in cyber

[2] Larry M. Wortzel, *The Dragon Extends its Reach: Chinese Military Power Goes Global* (Washington, DC: Potomac Books, 2013), pp, 17, 41-41, 134, 145-148.
[3] Dan Mcwhorter, "APT1 Three Months Later – Significantly Impacted, Though Active & Rebuilding," *M-Unition* (May 21, 2013). *https://www.mandiant.com/blog/apt1-months-significantly-impacted-active-rebuilding/.*
[4] William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, (London and New York: Routledge, 2013), p. 226.

espionage activities, China's Ministry of Foreign Affairs insisted China is "strongly against any form of hacking activities," and dismissed such charges as "baseless."[5]

I believe that regardless of the evidence that is presented, Chinese Communist Party leaders will continue to deny that the People's Liberation Army (PLA) and other government and intelligence organizations are behind these penetrations. After all, this is the same party and government that deny that anyone was killed in Tiananmen Square when the Chinese military massacred about 2,500 people in June 1989.[6]

However, a number of public U.S. government reports, admissions by private companies that they have been the target of cyber espionage, investigations by cyber security firms, and U.S. press reports contradict Beijing's longstanding denials. There is now evidence that the Chinese government not only is encouraging and shaping these attacks, but also directing and executing them. While attribution is difficult and takes great skill, trend analysis is allowing cyber security professionals to develop a more comprehensive understanding of Chinese cyber actors, tools, tactics, techniques, and procedures.

Threats to U.S. National Security

China's cyber espionage against the U.S. government and defense industrial base poses a major threat to U.S. military operations, the security and well-being of U.S. military personnel, the

[5] Don Lee, "China Dismisses U.S. Accusations of Cyber-Spying," *The Los Angeles Times*, May 07, 2013. *http://articles.latimes.com/2013/may/07/world/la-fg-wn-china-us-cyber-spying-20130507.*
[6] Larry M. Wortzel, "The Tiananmen Massacre Reappraised: Public Protest, Urban Warfare, and the People's Liberation Army," in Andrwe Scobell and Larry M. Wortzel, eds., *Chinese National Decisionmaking Under Stress* (Carlisle,PA: Strategic Studies Institute, 2005), pp. 55-84.

effectiveness of equipment, and readiness. China apparently uses these intrusions to fill gaps in its own research programs, map future targets, gather intelligence on U.S. strategies and plans, enable future military operations, shorten research and development (R&D) timelines for military technologies, and identify vulnerabilities in U.S. systems and develop countermeasures.[7]

Military doctrine in China also calls for attacks on the critical infrastructure of an opponent's homeland in case of conflict, which explains some of the Chinese cyber penetrations in the U.S.[8] One senior researcher at the Chinese Academy of Science said that in wartime, cyber warfare may disrupt and damage the networks of infrastructure facilities, such as power systems, telecommunications systems, and education systems in a country. Other PLA strategists have suggested that China should have the capability to paralyze ports and airports by cyber or precision weapon attacks on critical infrastructure.[9]

A number of instances of Chinese cyber espionage targeting U.S. national security programs have been identified in recent years:

- In a 2012 report to Congress on China's military power, DOD stated its networks are targeted about 50,000 times per year.[10] Although China is not responsible for all of these attacks, DOD has said China poses the dominant threat to its networks.[11] In its 2013 annual report to Congress, DOD for the first time explicitly accused China of committing

[7] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 166.
[8] Wortzel, *The Dragon Extends its Reach,* 142-145.
[9] Ibid., 145.
[10] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 154.
[11] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 155.

cyber espionage. The report states China is using cyber operations to "support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors."[12]

- In 2012, the National Aeronautics and Space Administration (NASA) disclosed a cyber intrusion into NASA's Jet Propulsion Laboratory network originating from China-based Internet protocol (IP) addresses. According to NASA, the intruders gained "full, functional control" over the network, enabling them to copy, delete, or modify sensitive files; manipulate user accounts for mission-critical systems; and steal user credentials to access other NASA systems.[13]

- A number of U.S. press reports indicate that since as early as 2007 Chinese cyber operators have repeatedly infiltrated the networks of the F-35 Joint Strike Fighter's major contractors – Lockheed Martin, Northrop Grumman, and BAE Systems – and stolen aspects of its design plans.[14] Some experts, noting the resemblance between China's newest stealth fighter, the J-31, and the F-35, have suggested the J-31 was developed using F-35 design plans.[15]

---

[12] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: Department of Defense, 2013), p. 36.
[13] House Committee on Science, Space, and Technology Subcommittee on Investigations and Oversight, *Hearing on NASA Cybersecurity: An Examination of the Agency's Information Security*, testimony of Inspector General Paul K. Martin, 112th Cong., 2nd sess., February 29, 2012.
http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf.
[14] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 155.
[15] Trefor Moss, "China's Stealth Attack on the F-35," *The Diplomat*, September 27, 2012.
http://thediplomat.com/flashpoints-blog/2012/09/27/the-fake-35-chinas-new-stealth-fighter/.

- U.S. press reporting indicates that, beginning in 2007, Chinese cyber actors appear to have infiltrated the networks of QinetiQ, a defense contractor specializing in military robotics, satellites, and combat helicopter technology. Undetected for several years, the hackers stole millions of pages of sensitive research documents, and used QinetiQ as a back door into U.S. military networks. In 2012, the PLA released a bomb disposal robot with characteristics similar to one of QinetiQ's designs.[16]

- In May 2013, *The New York Times*, citing a classified report by the Defense Science Board, stated that over several years Chinese cyber actors have compromised the designs of more than fifty sensitive U.S. technologies and advanced weapons systems, including the Patriot missile system, Aegis ballistic missile defense system, V-22 Osprey, F/A-18 fighter, and Littoral Combat Ship.[17]

Threats to U.S. Industry

China's cyber espionage against U.S. commercial firms poses a significant threat to U.S. business interests and competiveness in key industries. General Keith Alexander, commander of U.S. Cyber Command, assessed that the financial value of these losses is about $338 billion a year, including intellectual property losses and the down-time to respond to penetrations,

[16] Michael Riley and Ben Elgin, "China's Cyberspies Outwit Model for Bond's Q," *Bloomberg*, May 2, 2013. *http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html.*
[17] Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *New York Times*, May 27, 2013. *http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html#.*

although not all those losses are to Chinese activity.[18] Chinese entities engaging in cyber and other forms of economic espionage likely conclude that stealing intellectual property and proprietary information is much more cost-effective than investing in lengthy R&D programs.[19] These thefts support national science and technology development plans that are centrally managed and directed by the PRC government.

The Chinese government, including the PLA and the Ministry of State Security, supports these activities by providing state-owned enterprises (SOEs) information and data extracted through cyber espionage to improve their competitive edge, cut R&D timetables, and reduce costs. The strong correlation between compromised U.S. companies and those industries designated by Beijing as "strategic" industries[20] further indicates a degree of state sponsorship, and likely even government support, direction, and execution of Chinese economic espionage.[21] Such governmental support for Chinese companies enables them to out-compete U.S. companies, which do not have the advantage of leveraging government intelligence data for commercial gain.[22]

---

[18] Josh Rogin, "NSA Chief: Cybercrime Consitutues the 'Greatest Transfer of Wealth in History'," *Foreign Policy: The Cable*, July 9, 2012, *http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history*

[19] Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery is a National Policy – And Must Be Challenged," *Wall Street Journal*, January 27, 2012. *http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html.*

[20] The Commission on the Theft of Intellectual Property, *The IP Commission Report*, (Washington, DC: National Bureau of Asian Research, May 2013), p. 12. *http://ipcommission.org/report/IP_Commission_Report_052213.pdf.*

[21] U.S.-China Economic and Security Review Commission, *2012 Annual Report to* Congress (Washington, DC: U.S Government Printing Office, November 2012), p. 156.

[22] In the late 1980s and early 1990s a debate took place in Congress on whether the U.S. Intelligence Community (IC) should share information and/or intelligence assets with U.S. companies to provide those companies an advantage against foreign competitors. In 1991, Director of the Central Intelligence Agency Robert Gates, in a speech to the IC, stated clearly that the CIA would limit itself to helping U.S. companies safeguard themselves from foreign intelligence operations. Robert Gates, "The Future of American Intelligence," (Washington, DC: U.S. Intelligence Community, December 4, 2011).

It is difficult to quantify the benefits Chinese firms gain from cyber espionage. We don't know everything about the kinds of information targeted and taken, nor do we always attribute theft to a specific Chinese actor. Some thefts may never be detected. In terms of business intelligence, some targets of cyber-theft likely include information related to negotiations, investments, and corporate strategies including executive emails, long-term business plans, and contracts. In addition to cyber-theft, Chinese companies almost certainly are acquiring information through traditional espionage activities, which limits our ability to identify the impact of cyber espionage in particular. Nevertheless, it is clear that China not only is the global leader in using cyber methods to steal intellectual property, but also accounts for the majority of global intellectual property theft.[23] Chinese actors have on several occasions in recent years leveraged cyber activities to gain sensitive or proprietary information from U.S. enterprises:

- In June 2013, the Department of Justice filed charges against a Chinese energy firm, Sinovel Wind Group, alleging it stole secrets from AMSC (previously American Superconductor Corporation). In 2005, the two companies partnered together, leveraging AMSC's high-technology components and Sinovel's specialization in low-cost manufacturing. Once Sinovel was able to reproduce AMSC's technology after stealing its proprietary source codes, the Chinese firm broke the partnership, cancelled existing orders, and devastated AMSC revenue. AMSC later filed several lawsuits in Chinese courts, where Sinovel's assets are located. While the case continues to move slowly

[23] The Commission on the Theft of American Intellectual Propoerty, *The IP Commission Report* (Washington, DC: May 2013), pp. 3, 18. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.*

through the Chinese legal system, adding to AMSC's legal fees, Sinovel is reaping the profits of stolen technology.[24]

- In 2013, Mandiant, a private cyber-security firm, provided detailed technical information tracing the activities of a known cyber threat group, APT1, to a building believed to house the PLA's 2nd Bureau of the General Staff Department's Third Department. According to Mandiant, the Third Department is responsible for conducting at least some of the PLA's computer network operations. Since 2006, the Third Department's Shanghai-based 2nd Bureau committed at least 141 network intrusions across fifteen countries and twenty major industries, from information technology to financial services. 81 percent of the victims were organizations either located in the United States or with U.S.-based headquarters. Mandiant concludes the unit receives "direct government support."[25]

- Aside from its 2nd Bureau in Shanghai, the PLA Third department has another eleven operational bureaus, three research institutes, four operations centers, and sixteen technical reconnaissance units in military regions with operational forces.[26] Not all of these are directing their actions against the United States, and there are no public reports available about what cyber espionage they may have conducted like the Mandiant report about the 2nd Bureau.

---

[24] Melanie Hart, "Criminal Charges Mark New Phase in Bellweather U.S.-China Intellectual Property Dispute," *Center for American Progress*, June 27, 2013. *http://www.americanprogress.org/issues/china/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/.*

[25] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 2013, pp. 22-23. *http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.*

[26] United States Department of Defense, *Directory of PRC Military Personalities* (Washington, DC: Defense Intelligence Agency, March 2013), *passim.*

- In an October 2011 report, the U.S. Office of the National Counterintelligence Executive (ONCIX) linked multiple cyber intrusions and instances of intellectual property theft to Chinese individuals or China-based computer systems. The report concludes the "growing interrelationships between Chinese and U.S. companies...will offer Chinese government agencies and businesses increasing opportunities to collect sensitive U.S. economic information."[27]

- In 2011, McAfee, a U.S.-based internet security firm, detailed a series of "covert and targeted cyber [attacks]," dubbed "Night Dragon." Originating primarily from servers in China, "Night Dragon" targeted oil, energy, and petrochemical companies in the United States and other countries, ultimately gaining access to executive accounts and highly sensitive documents over several years.[28]

- Also in 2011, McAfee detailed the activities of "Operation Shady RAT," a cyber actor that compromised data from 49 U.S. entities, including defense contractors, energy companies, real estate companies, and information and communications technology firms, among others.[29] Following the publication of McAfee's report, several security experts asserted that "Operation Shady RAT" was a Chinese government operation.[30]

---

[27] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, (Washington DC: October 2011), *http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.*
[28] McAfee, *White Paper: Global Energy Cyberattacks: 'Night Dragon'* (Santa Clara, CA: McAfee Foundstone Professional Services and McAfee Labs, February 10, 2011), p. 4. *http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.*
[29] Dmitri Alperovich, *Revealed: Operation Shady RAT* (Santa Clara, CA: McAfee, August 2011). *http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.*
[30] Laura Saporito and James A. Lewis, "Cyber Incidents Attributed to China," Center for Strategic and International Studies. *http://csis.org/files/publication/130314_Chinese_hacking.pdf.*

- The PLA in 2009 may have conducted a "spearphishing" campaign against the Coca-Cola Corporation. The alleged attack coincided with Coca-Cola's attempts to acquire China Huiyuan Juice Group for $2.4 billion, which would have been the largest foreign takeover of a Chinese company. Hackers gained access to sensitive corporate documents, presumably targeting Coca-Cola's negotiation strategy. Shortly after the FBI informed Coca-Cola that its network was compromised, the acquisition collapsed.[31]

Outlook

There is an urgent need for Washington to compel Beijing to change its approach to cyberspace and deter future Chinese cyber theft. The Chinese government does not appear to be inclined to curb its cyber espionage in any substantial way. Merely naming perpetrators will not affect this centrally directed behavior.

Later this week, the U.S.-China Economic and Security Review Commission will hold a roundtable with leaders in the cyber security field to explore a range of potential Congressional actions and policies, including the following:

- Expose China's illicit behavior in cyberspace and present detailed evidence of Chinese cyber espionage. Jason Healey, director of the Cyber Statecraft Initiative at the Atlantic

[31] David E. Sanger et al., "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *New York Times*, February 19, 2013. *http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?hp&_r=0&pagewanted=all*; Ben Elgin et al., "Coke Gets Hacked and Doesn't Tell Anyone," *Bloomberg*, November 4, 2012. *http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html.*

Council, recently suggested that the U.S. government should task the intelligence community to release periodic reports detailing Chinese espionage.[32]

- Link Chinese economic espionage to trade restrictions and bilateral issues in which Beijing seeks compromises from Washington. The *Deter Cyber Theft Act* (S. 884), a bi-partisan bill recently introduced in the U.S. Senate, would allow the President to restrict the import of specific goods in order to protect intellectual property rights and DOD supply chains, and require further study of foreign industrial espionage.

- Encourage the U.S. government, military, and cleared defense contractors to implement measures to reduce the effectiveness of Chinese cyber operations and increase the risk of conducting such operations for Chinese organizations. For example, measures such as "meta-tagging, watermarking, and beaconing"[33] can help identify sensitive information and code a digital signature within a file to better detect intrusion and removal.[34] These tags also might be used as evidence in criminal, civil, or trade proceedings to prove that data was stolen.

- Continue or expand bilateral cooperation with China on credit card and bank crime.

---

[32] Jason Healey, "How the U.S. Should Respond to Chinese Cyberespionage," *New Atlanticist Policy and Analysis Blog*, Atlantic Council, February 25, 2013. *http://www.acus.org/new_atlanticist/how-us-should-respond-chinese-cyberespionage.*

[33] The Commission on the Theft of Intellectual Property, *The IP Commission Report* (Washington, DC: National Bureau of Asian Research, May 2013), p. 81. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.*

[34] Cisco, "Data Loss Prevention," *http://www.cisco.com/en/US/netsol/ns895/index.html.*

- Prohibit Chinese firms using stolen U.S. intellectual property from accessing U.S. financial markets. As recommended by the Commission on the Theft of Intellectual Property in its 2013 report, the U.S. Secretary of the Treasury and Secretary of Commerce could be empowered to "deny the use of the American banking system to foreign companies that repeatedly benefit from the misappropriation of American intellectual property."[35]

- Prosecute or punish firms that benefit from cyber-theft, regardless of whether or not they are involved in specific cyber espionage. Companies may not be willing to cooperate with Chinese cyber actors if it means risking civil and criminal litigation and frozen assets.[36]

My personal view is that the President already has an effective tool that he has not used. General Alexander put the annual cost of cyber theft at $338 billion a year. To put that number in perspective, a new *Gerald R. Ford*- class aircraft carrier costs about $12 billion. Given the magnitude of these losses, the President could employ his authority under the International Emergency Economic Power Enhancement Act (IEEPA, 50 USC 1701, PL 110-96) to declare that the cyber-enabled theft of intellectual property represents an "extraordinary threat to the national security…or economy of the United States."

---

[35] The Commission on the Theft of Intellectual Property, *The IP Commission Report* (Washington, DC: National Bureau of Asian Research, May 2013), p. 66.
http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
[36] Stewart Baker, "The Attribution Revolution," *Foreign Policy*, June 17, 2013.
http://www.foreignpolicy.com/articles/2013/06/17/the_attribution_revolution_plan_to_stop_cyber_attacks?page=full.

Under this declaration, the President, in consultation with Congress, may investigate, regulate, and freeze transactions and assets, as well as block imports and exports in order to address the threat of cyber theft and espionage. While this authority has traditionally been employed to combat international financing of terrorist organizations and the proliferations of weapons of mass destruction, there is no statutory limitation that prevents the President from applying the IEEPA to cyber espionage issues.[37]

This committee's job is made harder by the reluctance of companies to admit that cyber theft has taken place. The government and industry must work more closely to detect cyber penetrations and to respond. No interagency effort can monitor intrusions on every corporate network. But the government and industry can do better at detecting and responding to cyber theft.

Thank you for the opportunity to appear today. I am happy to respond to any questions you may have.

[37] 50 U.S.C. § 1701. *http://uscode.house.gov/download/pls/50C35.txt.*

Mr. MURPHY. Mr. Lewis, you are recognized for 5 minutes.

STATEMENT OF JAMES A. LEWIS

Mr. LEWIS. Thank you, chairman. And thank you for the committee's opportunity to testify. I feel right at home, since I was born in Pittsburgh and lived in Evanston. So it's good to be back.

I should note that one of the things I do is lead track 2 discussions with government agencies in China. We've had eight meetings that have included the PLA, the Ministry of State Security, and others. Some of my testimony is based on this not-public information. I'm going to discuss three issues: Why China steals intellectual property, what the effects of this are in the U.S. and China, and steps we can take to remedy the problem.

Cyber espionage is so pervasive that it challenges Beijing's ability to control it. Every Fortune 500 company in the U.S. has been a target of Chinese hackers, in part because American defenses are so feeble. Right? China has four motives for cyber espionage: First, they have an overwhelming desire to catch up and perhaps surpass the West. Second, they believe that rapid economic growth is crucial for the party to maintain its control. Third, they have no tradition of protecting intellectual property. And, finally, some Chinese leaders fear that their society has lost the ability to innovate and the only way to compensate is to steal technology. China supports its strategic industries and state-owned enterprises through cyber espionage. For example, China's economic plans made clean energy technology a priority, and the next thing that happened was the clean energy companies in the U.S. and Germany became targets.

China's economic espionage activities against the U.S. are greater than the economic espionage activities of all other countries combined. The effects, however, are not clear-cut benefits for China. China often lacks the know-how and marketing skills to turn stolen technology into competing products. A dollar stolen does not mean a dollar gained for China. This is not true for confidential business information, which a director of an allied intelligence service once described as normal business practice in China. So if you're going to negotiate, if you're going for business, they will steal your playbook; they will know your bottom line. This is immense, immediate advantage. But cyber espionage also hurts China. One of their goals is to become an innovative economy. And they are unable to do this while they are dependent on espionage. They also create immense hostility and suspicion in their relations with many countries. The U.S. is not the only victim.

Espionage is a routine practice among great powers. And no one can object to espionage for military and political purposes. What is unacceptable is espionage for purely commercial purposes. Frustration with the lack of progress in discussions with China have led to suggestions for sanctions or retaliation. These are not in our interest. We don't want to start a war with China, nor do we want to crash the Chinese economy. Hacking back has little real effect and runs contrary to U.S. law and international commitments.

Instead, we need a strategy with four elements. Sustained high-level attention. This is going to take years. This is not something we're going to fix in a couple of months. We need to create public

disincentives for the Chinese hacking, using Treasury, visa laws, and perhaps FBI activities, Department of Justice activities. We need closer coordination with our allies, most of whom are not on the same page as us in this matter. And, finally, we need improved cyber defenses to make our companies stronger.

Last month, a U.N. Group that included the U.S. and China said that international law and the principles of state responsibility apply to cyberspace. This agreement provides a foundation for rules on hacking. The best strategy, the one that has the best chance of success, is to create with our allies global standards for responsible behavior and then press China to observe them. To use a favorite Chinese expression, we want a win-win outcome rather than a zero-sum gain where only one side can win.

Cyber espionage lies at the heart—the heart of the larger issue of China's integration into the international system, and at the heart of the efforts of the Chinese to modernize their economy. This is a problem that has become one of the leading issues in international relations. China's economic growth has been of immense benefit to the world. But what was tolerable when China was an emerging economy is no longer tolerable when it is the world's second largest economy. I think we are on the path to resolving this issue, but it is a path that will take many years to complete. And I thank the committee for its attention to this issue. I look forward to your questions.

Mr. MURPHY. Thank you, Mr. Lewis.

[The prepared statement of Mr. Lewis follows:]

Testimony
Cyber Espionage and the Theft of U.S. Intellectual Property and Technology
Committee on Energy and Commerce
U.S. House of Representatives
July 9, 2013
James A. Lewis, Center for Strategic and International Studies

I thank the Committee for the opportunity to testify on this important subject. The hearing is particularly timely coming as it does at the same time as the Strategic and Economic Dialogue between U.S. and Chinese leaders. I will discuss three issues in my testimony: why China steals intellectual property; what the effects of this are on the U.S. and on China; and steps we can take to remedy this problem.

Chinese officials are concerned that disputes over cybersecurity could become a major problem in the bilateral relationship. They are interested in gauging the extent of U.S. concern and finding ways to assuage it. That said, they appear unwilling, absent significant pressure, to give up the long-running national effort to illicitly acquire technology from Western companies. Chinese economic espionage has moved into cyberspace, is now part of normal business practice, reflects deeper problems with the protection of intellectual property, and is so pervasive that it will take years of sustained effort to bring it under control. While an immediate solution is impossible, there must be evidence of progress to avoid further damage to bilateral relations and to reduce a troubling source of instability in international affairs.

Why China Steals Intellectual Property

The Chinese leaders who succeed Mao Zedong in 1978 knew that his policies had left their country in desperate shape. It was impoverished, technologically backward, and falling further beyond most other countries. In a bold move, they decided to open their previously closed nation to western investment. A key part of this opening was China's intention to acquire western technology by licit and illicit means. This acquisition of technology has been part of China's economic strategy for more than thirty years. The foreign investment that flooded into China when its economy opened presented a tremendous opportunity. Foreign firms entering China were pressed in the approval process to transfer technology through joint ventures, in contract negotiations or licensing agreements, or through investment in research facilities in China.

Interviews with numerous companies identify a consistent pattern of behavior. Companies report that technology transfer concessions are a part of business negotiations in China, to provide an advantage to Chinese firms. Chinese regulations and policies can restrict the ability of a foreign company to make Chinese partners agree to confidentiality agreements to safeguard technology or to restrict sales of derivative products. Western firms complain that regulations skew technology transfers in favor of Chinese firms. Companies cite risk to IP, along with regulatory uncertainty, as the two major obstacles to doing business in China. China has relied on the appeal of its growing market to overcome investor reluctance, but there are signs that foreign firms are reconsidering the risks as Chinese firms try to export their own high-tech products to the rest of the world.

There are four reasons that China seeks to acquire technology by any means possible. First, they have an overwhelming desire to catch up with and to surpass the West. Second, they believe that rapid economic growth is politically essential for the party to maintain its dominance. Third, China has no tradition of protecting intellectual property and thirty years of Maoism only made things worse. Finally, the Chinese fear that they have lost the capability to innovate and must depend on stolen technology. In combination, these motives mean that it will be very difficult to get China to change its behavior.

American companies first thought they could control the risk of the theft of intellectual property in China. Most believe that the damage from espionage is part of the cost of doing business in the world's fastest growing markets, and that American companies can create new technologies faster than their competitors can bring the old ones to market and so minimize any loss. Companies used a variety of techniques that would prevent Chinese competitors from getting access. These include holding back key processes from Chinese employees, allowing access only to lower-end technologies, keeping advanced functions outside China, and monitoring employee activities. These strategies provide some protection, but their chief flaw is that they were designed for a pre-internet world. Leaving essential plans stored on a company computer in the U.S. no longer protects them from theft when that computer is connected to the global internet.

The internet makes espionage easier – something we have all come to appreciate in recent weeks. This includes the theft of intellectual property and trade secrets. To give an example, in the mid 1990s an American aircraft manufacturer had an assembly plant in Shanghai. When the American company put surveillance cameras in the ceiling, they discovered that Chinese agents were coming into the plant every night to take things apart, and photograph and copy machinery and plans. The internet provides a new avenue for illicit acquisition. In a more recent case, Chinese hackers simply downloaded blueprints by hacking into the aircraft manufacturer's computers. This is simpler, faster, and more complete. China's economic espionage has moved into cyberspace, is part of normal business practice, reflects deeper problems with the protection of intellectual property, and is so pervasive as to challenge Beijing's ability to control it.

We also need to recognize that many companies have not paid serious attention to securing their networks. There is no obvious incentive for them to do so. This means that it is very easy for Chinese hackers to extract intellectual property from companies in the U.S. and around the world. Once the Chinese discovered this – about a decade ago when global high-speed networks became common, they were quick to exploit the opportunity to move their existing economic espionage programs into cyberspace.

Companies know that their IP is at risk in China but many still estimate that the risk of technology loss is outweighed by economic opportunity. There is an economic rationale for this, in that near term gain for an individual firm outweighs long-term costs, particularly if it takes five years or more for a competing product to appear. But several dubious assumptions underlie this rationale. The illicit acquisition of technology, even if the technology is dated by U.S. standards, helps build Chinese industries and accelerates military modernization. It accelerates improvement in indigenous industrial and technological capabilities, making the recipient better

able to absorb stolen technology and faster at creating competitive products. Companies have underestimated the risk they face, and every Fortune 1000 company in the U.S. has been a target for Chinese hackers who, in many cases, have succeeded in gaining entry and exfiltrating information.

Chinese interlocutors use a variety of reasons to justify these actions. They cite the "Century of Humiliation" when China was carved up by European powers, or the still-overwhelming poverty of many Chinese and the need for growth. Some will say that the U.S. engaged in similar activities in the 19th century when it was a growing economy. None of these excuses makes any sense. The real justification is that China believes it has no choice - politically, economically and militarily - but to take foreign technology.

The Harm to the U.S. and to China

Many discussions of cybersecurity invariably involve exaggeration. The source of this exaggeration is often a lack of specificity in precisely assessing intent, capabilities, and effect. This lack of precision leads to policy recommendations that are either pointless or frivolous. China has the intent to steal intellectual property and its capabilities are more than adequate since American defenses are feeble. China's economic espionage activities against the United States are greater than the economic espionage activities are of all other countries combined. The effect, however, is not one of clear-cut benefit to China. The strategic implications of this theft are difficult to assess. Some call it the greatest transfer of wealth in history; others call it a rounding error for an economy as big as that of the U.S. Neither characterization is correct.

First, it is difficult to estimate the value of intellectual property in the abstract, making it hard to come up with a precise estimate of the dollar value of the loss. Published estimates of the cost to the United States range from a few billion to hundreds of billion of dollars annually. CSIS and McAfee are undertaking a study on how to estimate the cost of all malicious cyber activity, including the theft of IP. Our current estimate is that the cost to the U.S. for all malicious cyber activity, including trade effects, job losses, insurance and recovery costs, fraud, and lost exports is less than 1% of America's GDP.

Second, to utilize stolen technology an opponent must accurately translate complex engineering terms from English to Chinese and then give it to someone with the necessary skills and access to a sufficiently sophisticated industrial base to make use of it. For China, there has been a lag of several years, perhaps as many as ten, between successful acquisition through espionage and the ability to produce competing products (be they military or civil). For simple technologies, it may only take a few months for the Chinese copy to appear; for complex technologies it can take up to a decade. One troubling trend is that this lag time between acquisition and the appearance of a competing product based on stolen technology is decreasing, as China's ability to absorb and utilize technology has increased.

There is no lag between acquisition and use when it comes to confidential business information, which can be used immediately. Theft of oil exploration data, sensitive business negotiation data, or even "insider" stock trading information can be used immediately to make money. The director of an allied intelligence service once described this theft of business confidential

information as a "normal business practice" in China.

China has carefully studied how the U.S. uses technology to increase its military capabilities and has targeted these technologies for acquisition – stealth technology is the best-known example. Chinese espionage has also focused on anti-access capabilities, to deny the U.S. the ability to intervene effectively in Asia. China also takes seriously the discussion in the U.S. of an "Air-Sea Battle" between the U.S. and had undertaken cyber espionage to gain access to relevant technologies, not only to copy them but also to study how they work, in order to be able to neutralize them in combat.

We know that state-sponsored espionage will focus on areas of concern to governments: military and advanced technologies in aerospace, materials, information technology, and sensors, financial data and energy related information. Semiconductors and solar energy have been prime targets. However, government hackers from the PLA and other agencies also engage in cyber espionage as a moneymaking activity and Chinese companies make use of private hackers for purposes of commercial espionage. Private hackers, if they are good, are invited by their local Security Bureau to visit and "drink tea," during which it is suggested that they cooperate in going after certain targets. There is no possible national security benefit to this kind of theft and this is where China's behavior is objectionable.

Most companies prefer to conceal the loss of intellectual property to Chinese hacking, but a few cases have emerged to illustrate its scope. Perhaps the most famous involves Google and several dozen other companies hacked a few years ago – most did not admit publicly to their losses. The Google case illustrates the blend of motives that make Chinese cyber espionage so complex. Chinese hackers looked for information on political dissidents n Gmail. They also examined Gmail to see if the FBI was monitoring the accounts of Chinese agents in the United States. These are legitimate state activities, but the Chinese also took intellectual property related to Google services and products, such as search engine technology, and passed this information to Google's Chinese competitors, an action that violated China's trade commitments to the WTO and to the U.S.

A number of other cases have come to light, including technology taken from Cisco, Nortel, and Motorola – of these only Nortel involved cyber espionage. The current indictment of Chinese competitors for taking technology from Sinovel and American Semiconductor also point to a common pattern. The Chinese government made clean energy technology a priority and clean energy companies in the U.S. became targets. A similar pattern can be detected for the automotive industry and high-speed trains (from Germany and Japan). It is safe to assume that classified information could identify many more cases of U.S. companies that have lost IP to Chinese hackers. China supports its 'strategic industries" identified in China's economic planning and its State-Owned Enterprises through cyber espionage.

The tasking of Chinese espionage and the identification of targets appears to be a diffuse process. There may be general guidelines issued by Beijing, but hackers from the PLA or other Ministries seem to have a great deal of freedom in targeting and in responding to requests for favored companies or research institutions. There are collection targets set by China's military strategy or economic plans, collections to support specific company or military acquisition projects, and

targets of opportunity, where Chinese hackers penetrate a system, come across IP they think is valuable and then transfer or sell it to a favored company.

Chinese claims that the U.S. also engages in economic espionage are ridiculous, if for no other reason that there is little Chinese technology worth stealing. To argue that the U.S. should not object to espionage by China as we did this to Britain is inane – the scale is in no way comparable. The U.S. government did not steal (and does not steal) commercial technology to give to its companies. In addition, the U.S. was a net contributor to the global stock of knowledge in the 19th century, with its citizens creating steamboats, the telegraph, the cotton gin, and countless other inventions that other nations copied freely. The current perpetrators of economic espionage have made no such contribution.

Espionage for national security purposes is a routine aspect of relations among great powers. What is unacceptable is espionage for purely commercial purposes. All great powers engage in espionage against military and political targets. China is no different from any other large nation in doing this, including the United States. Where China's espionage efforts differ significantly from international practice is in the rampant economic espionage carried out by Chinese government entities, including the PLA. Both the U.S. and China would agree that espionage is appropriate to protect national security and advance national interests. Where they would differ is that China sees economic espionage as a legitimate activity to advance its security and interests by securing the technology needed for growth and military power. The broad range of collection targets reflects an official policy to encourage the illicit acquisition of technology as a way to promote economic growth and to modernize China's military forces.

There is also a link between cyber espionage and the development of cyber attack capabilities. Cyber espionage provides, if nothing else, knowledge of potential targets and training for potential attackers. There is also a link between cyber espionage directed at commercial targets and cyber espionage targeted on military technology. It is often the same actors pursuing a collection plan that targets both military and commercial sources – the penetration of RSA was commercial espionage undertaken to enable the penetration of military industrial targets. This report was not tasked with estimating the effect of cyber espionage on U.S. military superiority but a strong case could be made that there has been extensive damage to the U.S. lead in stealth, submarine, missile and nuclear capabilities. We cannot accurately assess the dollar value of the loss in military technology but cyber espionage, including commercial espionage, shifts the terms of engagement in China's favor.

The most troubling aspect of this espionage is that State actors in China, such as the PLA, engage in espionage for reasons of profit. PLA units find commercially valuable information in their quest for military technology and then sell it to Chinese companies. State Owned enterprises can request help from PLA units to hack into a target company's network and then compensate. Many of these activities are outside of Beijing's control, sponsored by politically powerful regional party officials or commanders. This raises the political cost to President Xi of any effort to clamp down. It will also be difficult to change Chinese behavior because if President Xi asks the PLA to stop hacking, he is essentially asking them to stop making money through an activity that many Chinese see as justified. National strategies, politics, and business all combine to make hacking foreign companies to steal technology an attractive proposition.

China is also damaged by the theft of trade secrets and economic espionage. Chinese companies are also victims of hacking by their Chinese competitors. One reason China has no major software company is that no software product can capture market share in a climate of rampant IP theft and piracy. This points to a fundamental tension in Chinese. China is pursuing two contradictory goals. China wants to move up the "value chain of production and, rather than merely assembling other peoples technology, be able to create its own. While much of the technology we use today is assembled in China, it is designed in other nations (principally the U.S., Japan and Germany) and the bulk of the profits go to non-Chinese companies. China is in fact a net importer of technology. It is a long-standing goal of China's leadership to change this, but unchecked cyber espionage undercuts their efforts to create indigenous innovation.

There is an unspoken concern among Chinese policy makers that China does not have the ability to innovate. This is a complex topic best reserved for another discussion but China's "state capitalism" model and its one-party politics likely impedes innovation. Chinese outside of China have no problem innovating, but China's political system and its role in economic decision-making seems to have a chilling effect. China has been willing to invest vast resources to create a national science and technology base capable of supporting innovation far more consistently than the United States, but the political cost of "indigenous innovation" is immense and the pace of change in innovation capabilities may be linked to the pace of political reform.

Discussions with Chinese officials and companies suggest that there is a growing realization in Beijing and elsewhere that weak IP protection is a disincentive to innovation by the Chinese themselves. Some Chinese officials worry that a closed, "techno-nationalist" approach will damage innovation. The emphasis on "indigenous innovation" as it becomes another policy aimed at boosting China's creation of IP that has not delivered adequate results. They realize that they will eventually have to protect intellectual property to help their own companies and their own economy.

Changing China's Behavior

Chinese leaders realize that they face conflicting domestic goals and a serious bilateral problem. Economic espionage provides a technology boost, but puts bilateral relations with the U.S. at risk and hampers China's ability to create indigenous innovation. So far, China has been unwilling to give up its long-running national effort to illicitly acquire technology from Western companies, but action and engagement on this issue by the U.S. and other nations could change calculations of cost and benefit by Chinese leaders.

It is not useful to think of this issue in terms of confrontation, punishment, or conflict. We need a long-term diplomatic strategy linked to our larger goals for Asia and the world. Frustration with the lack of progress in stemming China's activities has led to a variety of bellicose suggestions, few of which make any sense and some of which could actually harm the United States. It is not in our interest to start a military conflict with China, nor is it in our interest to crash the Chinese economy – something that would unleash another global recession. Similarly, a trade war could do more damage to the American economy than cyber-espionage. Hacking back has little real effect, holds real risk of unintended damage, and could start an inadvertent

conflict with China, as the Chinese believe that the U.S. government endorses any private action by Americans. Hacking back runs contrary to U.S. international commitments and to the larger U.S. strategy for making cyberspace more secure.

This is not a new Cold War. We cannot have a Cold War with one of our largest trade partners. The two economies are too intertwined to go back to the rigid, bipolar separation we had with the Soviet Union. There are elements in each country that define the relations in terms of military competition, particularly in the PLA, and Chinese society can be prone to fits of hyper-nationalism, but if China wants to continue to grow and if the U.S. wants to remain a global leader, we have to find ways to cooperate. This will be a difficult process and cyber espionage has become a flashpoint in the relationship.

What the U.S. needs is a broad strategy with four elements. These are a sustained, high level engagement with China on the theft of U.S. intellectual property; the development of measures that will increase U.S. leverage in the engagement process; close coordination with allies, all of whom also suffer from Chinese cyber espionage, to create norms of responsible behavior in cyberspace; and improved domestic cyber defenses to make our companies harder to pillage.

The domestic debate over cybersecurity has not been very useful. There is a tendency to substitute slogans and myths for facts in the discussion of cybersecurity. The result is that after six years of sustained effort by two administrations, we have made insufficient progress in hardening our networks, particularly commercial networks, in the face of Chinese cyber espionage and, of greater concern, Iranian preparations to attack U.S. critical infrastructure. It will be easier for China to give up commercial espionage if the cost of penetrating business networks is increased and the returns from those penetrations are minimized.

Similarly, the U.S. could reduce the risk of Chinese cyber espionage if it had an effective strategy for innovation and productivity growth. It is not that the pace of innovation in China (or any other BRIC nation for that matter) is speeding up. It is that the U.S. is slowing down, largely because of changes in government policy in both Congress and the Executive Branch. In theory, we could change this and reignite productivity growth and innovation. The core of an innovation strategy would be increased federal investment in science and technology and streamlining regulation and tax policy to remove impediments to productivity growth. This is unlikely to happen in the near term, but it remains a possibility. Renewed growth in innovation and productivity in the U.S. would lessen the strategic effect of Chinese cyber espionage.

Since it will be difficult for the U.S. to take the domestic measures needed to manage the risk of Chinese cyber espionage, our efforts now must focus on the diplomatic. In this area, there has been some progress. Last June, the U.S., China and other nations, as part of a UN Group of Government Experts (GGE) on Information Security endorsed the application to cyberspace of the UN Charter, international law, the principle of state responsibility, and national sovereignty. This included agreement that States would not use "proxies" for malicious cyber actions. We know that there are many steps between agreement and implementation when it comes to international practice, but at a recent Track II discussion in Beijing a Chinese official said in a reference to the GGE, that "China's position was evolving in the light of international experience." The U.S. has been working with other nations to build on the success of the GGE

to create norms and agreement on responsible state behavior in cyberspace. As this effort progresses, China's cyber espionage will be difficult to sustain.

Multilateral steps must be reinforced by bilateral work between the U.S. and China. We should expect this process to take years, given the domestic political problems China faces in reining in cyber espionage. In the upcoming Strategic and Economic Dialogue and its subsidiary working groups, we should first expect the Chinese to see if the creation of a working group on cyber issues is enough to placate the Americans – it is a standard ploy on diplomacy and politics to create a Commission to study a problem in order to bury it. They will test how much advantage over the U.S. they can get from the Snowdon revelations - they are unlikely to get much negotiating benefit from his revelation because the U.S. has always told China that military espionage is a two way street and that it is China's commercial espionage that creates problems. What we should expect from this first round is an agreed schedule and an agenda for future talks.

We can find a precedent for how to engage China on cyber espionage in the successful effort to engage China on nonproliferation in the 1990s. The U.S. and it allies created regimes and international norms that established that responsible states did not engage in proliferation. The U.S., supported by its allies, met regularly with Chinese officals to make this point, providing the Chinese with specific examples of objectionable behavior. Every senior US official who went to China made the point that the involvement of Chinese companies in proliferation must stop or it would harm China's relations with the rest of the world. Leaders from European countries, the European Union, and Japan, made the same point – this was particularly important as it demonstrated to the Chinese that this was not solely an American concern. Finally, at appropriate moments in the discussion, the U.S. was able to use or threaten to use a combination of sanctions, including Congressionally-mandated sanctions and other punitive measures to encourage progress.

During the course of discussion with China on economic espionage it may be necessary to consider similar measures, intended to provide leverage and impetus in the discussions, not to punish. The best course would be to use focused measures against individuals or companies identified as being involved in cyber espionage. These could include Treasury sanctions, visa restrictions, and potentially indictments or other trade measures. Any of these measures will face objections from some in the economic and trade communities, but being timid and legalistic will undercut our efforts to get China to change its behavior. At the same time, we need to avoid a rupture in relations or a disruption of trade. We want to encourage China's adherence to international law and agreements. China would benefit as well from better protection of intellectual property and closer adherence to WTO commitments if it wants a larger role in the global economy and its own innovation economy.

The engagement in the 1990s on proliferation is a useful model and evidence that China can be persuaded to change its behavior, but cyber espionage is a more difficult problem than proliferation. Larger economic issues are at stake for both China and the U.S. China is more powerful and more confident that it was two decades ago. Unless the U.S has been careful to build international support for norms of responsible behavior, punitive measures could backfire, and the pace of any discussion will be slower. Our fundamental strategy should be to set global standards for responsible state behavior and then persuade China to change its actions

accordingly. To use a favorite Chinese expression, we must see the talks as pursuing a "win-win" outcome rather than being a "zero sum" game, where for one side to win the other must lose.

The Chinese may be tempted to retaliate – you hear mutterings in China about banning Cisco or other American companies in retaliation for actions against Chinese firms - but it is not in China's interest to start a trade war or further strain bilateral relations. China's economy is weakening. Growth is slowing and China's leaders face a host of problems, including mis-investment, corruption, pollution, and unemployment. Official figures on the Chinese economy are inflated to conceal the extent of the problem. The last thing China need right now is a trade war with the U.S. Nor do the Chinese want to accelerate the trend of foreign investors avoiding the China market. The Chinese hold a significant amount of U.S. debt but it is naive to think this gives them an advantage. For one thing, where else would China put their money – certainly not in Europe or Japan or in their own economy, for that matter? We have to expect the Chinese to test U.S. resolve and must have adequate responses prepared and notified in advance to the Chinese. One element of any U.S. effort would be to warn the Chinese that such retaliation against U.S. firms is unacceptable and risks increased tensions between the two countries.

China's economic growth has been of tremendous benefit to the rest of the world. China has gained, but we have gained as much or more. But what was tolerable when China was an emerging economy is no longer tolerable within it is the world second largest economy. China's economic cyber espionage is a source of instability in the international community and increases the risk of conflict. Cyber espionage lies at the heart of the larger issue of China's integration into the international "system," the norms, practices and obligations that states observe in their dealing with each other and their dealings with the citizens of other states. China can list the justifications as to why it should not be held accountable, but a failure to hold China accountable for cyber espionage undermines efforts to get China to adhere to other international norms and commitments and to find a stable place for it in international relations.

This month's meeting of the Security and Economic Dialogue and its Cyber Working Group are an important first step, but they must be sustained and reinforced with a range of measures, including coordination with allies and improved domestic cyber defenses. Our goal should be sustained engagement to build a cooperative relationship with China that makes cyberspace more secure for all nations.

I thank the Committee for the opportunity to testify and look forward to you questions.

Mr. MURPHY. And now Ms. Offutt. Am I pronouncing that correctly? Thank you. You're recognized for 5 minutes.

STATEMENT OF SUSAN OFFUTT

Ms. OFFUTT. Thank you. Mr. Chairman, Ranking Member Schakowsky, members of the subcommittee, thank you for the opportunity to share our observations on the economic effects of intellectual property theft and efforts to quantify the impact of counterfeiting and piracy on the U.S. economy. Intellectual property plays a significant role in the U.S. economy, and the U.S. Is an acknowledged leader in its creation. Intellectual property is any innovation, commercial or artistic, or any unique name, symbol, logo, or design used commercially. Cyberspace, where much business activity and the development of new activities often take place, amplifies potential threats by making it possible for malicious actors to quickly steal and transfer massive quantities of data, including intellectual property, while remaining anonymous and difficult to detect. According to the FBI, intellectual property theft is a growing threat, which is heightened by the rise of the use of digital technologies. Digital products can be reproduced at very low costs, and have the potential for immediate delivery through the Internet across virtually unlimited geographic markets. Cyber attacks are one way that threat actors, whether they are nations, companies, or criminals, can target intellectual property and other sensitive information of Federal agencies and American businesses. While we have not conducted an assessment of the economic impact of cyber espionage, our work examining efforts to quantify the economic impact of counterfeited and pirated goods on the U.S. economy can provide insights on estimating economic losses.

Specifically, my testimony today addresses two topics: First, the economic significance of intellectual property protection and theft on the U.S. economy, and insights from efforts to quantify the economic impacts of counterfeiting and piracy on the U.S. economy. My remarks are based on two products that GAO issued over the past 3 years, a 2010 report on intellectual property, and 2012 testimony on cyber threats and economic espionage.

As reported in 2010, intellectual property is an important component of the U.S. economy. The U.S. economy and intellectual-property-related industries contribute a significant percentage to U.S. Gross domestic product. IP-related industries also pay higher wages than other industries and contribute to a higher standard of living in the United States.

Ensuring the protection of intellectual property rights encourages the introduction of innovative products and creative works to the public. According to the experts we interviewed and the literature we reviewed, counterfeiting and piracy have produced a wide range of effects on consumers, industry, government, and the aggregate national economy. For example, the U.S. economy may grow more slowly because of reduced innovation and loss of trade revenue. To the extent that counterfeiting and piracy reduce investments in research and development, companies may higher fewer workers and may contribute less to U.S. economic growth overall.

Furthermore, as we reported in 2012, private sector organizations have experienced data loss or theft, economic loss, computer intrusions, and privacy breaches. For example, in 2011, the media reported that computer hackers had broken into and stolen proprietary information worth millions of dollars from the networks of six U.S. And European energy companies.

Generally, as we reported in 2010, the illicit nature of counterfeiting and piracy makes estimating the economic impact of intellectual property infringement extremely difficult. Nonetheless, research in specific industries suggests the problem is sizable, which is a particular concern, as many U.S. industries are leaders in the creation of IP. Because of difficulty in estimating the economic impacts of these infringements, assumptions must be used to offset the lack of data. Efforts to estimate losses involve assumptions, such as the rate at which consumers would substitute counterfeit for legitimate goods, and these assumptions can have enormous impacts on the resulting estimates. Because of the significant differences in types of counterfeit and pirated goods and industries involved, no single method can be used to develop estimates. Each method has limitations. And most experts observe that it is difficult, if not impossible, to quantify the economy-wide impacts. Mr. Chairman, Ranking Member Schakowsky, other members of the committee, this is the end of my statement. I'd be happy to answer questions.

Mr. MURPHY. Thank you. I appreciate that.

[The prepared statement of Ms. Offutt follows:]

United States Government Accountability Office

Testimony
Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at time 10:15 a.m.
EDT Tuesday, July 9, 2013

INTELLECTUAL PROPERTY

Insights Gained from Efforts to Quantify the Effects of Counterfeit and Pirated Goods in the U.S. Economy

Statement of Susan Offutt, Chief Economist

GAO-13-762T

GAO Highlights

Highlights of GAO-13-762T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

July 9, 2013

INTELLECTUAL PROPERTY

Insights Gained from Efforts to Quantify the Effects of Counterfeit and Pirated Goods in the U.S. Economy

Why GAO Did This Study

The United States is an acknowledged global leader in the creation of intellectual property. According to the Federal Bureau of Investigation, IP theft is a growing threat which is heightened by the rise of the use of digital technologies. IP is any innovation, commercial or artistic, or any unique name, symbol, logo, or design used commercially. IP rights protect the economic interests of the creators of these works by giving them property rights over their creations. Cyber attacks are one way that threat actors—whether nations, companies, or criminals—can target IP and other sensitive information of federal agencies and American businesses. While bringing significant benefits, increasing computer interconnectivity can create vulnerabilities to cyber-based threats. GAO was asked to testify on efforts to estimate the economic impacts of theft of intellectual property. Accordingly, this statement discusses (1) the economic significance of intellectual property protection and theft on the U.S. economy and (2) insights from efforts to quantify the economic impacts of counterfeiting and piracy on the U.S. economy. This statement is based on products GAO issued from April 2010 through June 2012 on the economic impacts of theft of intellectual property and on cyber threats and economic espionage.

What GAO Recommends

GAO is not making any new recommendations in this statement.

View GAO-13-762T. For more information, contact Susan Offutt at (202) 512-3763 or offuttsi@gao.gov.

What GAO Found

In April 2010, GAO reported that intellectual property (IP) is an important component of the U.S. economy and IP-related industries contribute a significant percentage to the U.S. gross domestic product. IP-related industries also pay significantly higher wages than other industries and contribute to a higher standard of living in the United States. Ensuring the protection of IP rights encourages the introduction of innovative products and creative works to the public. According to experts and literature GAO reviewed, counterfeiting and piracy have produced a wide range of effects on consumers, industry, government, and the economy as a whole. The U.S. economy as a whole may grow more slowly because of reduced innovation and loss of trade revenue. To the extent that counterfeiting and piracy reduce investments in research and development, companies may hire fewer workers and may contribute less to U.S. economic growth, overall. Furthermore, as GAO reported in June 2012, private sector organizations have experienced data loss or theft, economic loss, computer intrusions, and privacy breaches. For example, in February 2011, media reports stated that computer hackers had broken into and stolen proprietary information worth millions of dollars from the networks of six U.S. and European energy companies.

Generally, as GAO reported in April 2010, the illicit nature of counterfeiting and piracy makes estimating the economic impact of IP infringements extremely difficult. Nonetheless, research in specific industries suggests that the problem is sizeable, which is of particular concern as many U.S. industries are leaders in the creation of intellectual property. Because of the difficulty in estimating the economic impact of IP infringements, assumptions must be used to offset the lack of data. Efforts to estimate losses involve assumptions such as the rate at which consumers would substitute counterfeit for legitimate products, which can have enormous impacts on the resulting estimates. Because of the significant differences in types of counterfeited and pirated goods and industries involved, no single method can be used to develop estimates. Each method has limitations, and most experts observed that it is difficult, if not impossible, to quantify the economy-wide impacts.

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

Chairman Murphy, Ranking Member DeGette, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on cyber espionage and the theft of U.S. intellectual property and technology.

Intellectual property (IP) plays a significant role in the U.S. economy, and the United States is an acknowledged leader in its creation. IP is any innovation, commercial or artistic, or any unique name, symbol, logo, or design used commercially. IP rights protect the economic interests of the creators of these works by giving them property rights over their creations. The federal government grants IP protection through patents, copyrights, and trademarks, and takes enforcement actions that range from seizing IP-infringing goods to prosecuting alleged criminals.[1]

According to the Federal Bureau of Investigation, IP theft is a growing threat which is heightened by the rise of the use of digital technologies. The increasing dependency upon information technology systems and networked operations pervades nearly every aspect of our society. In particular, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While bringing significant benefits, this dependency can also create vulnerabilities to cyber-based threats. Cyber attacks are one way that threat actors—whether nations, companies, or criminals—can target the intellectual property and other sensitive information of federal agencies and American businesses. 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.

[1]In addition to copyrights, trademarks, and patents, two other IP protections are trade secrets and geographical indications. Trade secrets are defined as any type of valuable information, including a formula, pattern, compilation, program device, method, technique, or process that gains commercial value from not being generally known or readily obtainable; and for which the owner has made reasonable efforts to keep secret. Geographical indications are defined as indications that identify a good as originating in a country, region, or locality, where a given quality, reputation, or other characteristic of the good is essentially attributable to its geographic origin. Definitions used in this testimony for the various types of IP were provided by the U.S. Patent and Trademark Office.

While we have not conducted an assessment of the economic impact of cyber espionage, our work examining efforts to quantify the economic impact of counterfeited and pirated goods on the U.S. economy can provide some insights on estimating economic losses. Specifically in my testimony today, I will discuss (1) the economic significance of intellectual property protection and theft on the U.S. economy and (2) insights from efforts to quantify the economic impacts of counterfeiting and piracy on the U.S. economy.

My remarks are based on two previous GAO products issued from April 2010 through June 2012. For our April 2010 report assessing the economic impacts of theft of intellectual property on the U.S. economy, we interviewed officials and representatives from U.S. government agencies, industry associations, nongovernmental organizations, academic institutions, and a multilateral organization, and we reviewed documents and studies quantifying or discussing the impacts of counterfeiting and piracy on the U.S. economy, industry, government, and consumers.[2] We conducted a literature search of studies and estimates of the economic impact of IP infringements published since 1999 to examine various aspects of the economic impacts of counterfeiting and piracy, and to identify other insights about the role IP plays in the U.S. economy. We also interviewed subject matter experts from a range of governmental, nongovernmental, academic, and industry sources, and Organisation for Economic Cooperation and Development (OECD) officials to discuss efforts to quantify the economic impacts of counterfeiting and piracy and to obtain their views on the range of impacts of counterfeits and piracy, insights on counterfeiting activities and markets, and the role of IP in the U.S. economy. For background information on cyber threats, we relied on GAO's June 2012 testimony on cyber threats and economic espionage.[3] We conducted all of this work in accordance with generally accepted government auditing standards.

[2]GAO, *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*, GAO-10-423 (Washington, D.C.: April 12, 2010).

[3]GAO, *Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage*, GAO-12-876T (Washington, D.C.: June 28, 2012).

Background

Both government and private entities increasingly depend on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transmit sensitive and proprietary information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services. In addition, the Internet serves as a medium for hundreds of billions of dollars of commerce each year.

Cyberspace—where much business activity and the development of new ideas often take place—amplifies potential threats by making it possible for malicious actors to quickly steal and transfer massive quantities of data while remaining anonymous and difficult to detect.[4] Threat actors may target businesses, among others targets, resulting in the compromise of proprietary information or intellectual property. In addition, the rapid growth of Internet use has significantly contributed to the development of technologies that enable the unauthorized distribution of copyrighted works and is widely recognized as leading to an increase in piracy. Digital products are not physical or tangible, can be reproduced at very low cost, and have the potential for immediate delivery through the Internet across virtually unlimited geographic markets. Sectors facing threats from digital piracy include the music, motion picture, television, publishing, and software industries. Piracy of these products over the Internet can occur through methods including peer-to-peer networks, streaming sites, and one-click hosting services.

Economic Significance of Intellectual Property Protection and Theft

As we reported in April 2010, IP is an important component of the U.S. economy and IP-related industries pay higher wages and contribute a significant percentage to the U.S. economy. However, the U.S. economy as a whole may grow at a slower pace than it otherwise would because of counterfeiting and piracy's effect on U.S. industries, government, and consumers.

[4]Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (October 2011).

Importance of IP Has Long Been Recognized in the United States

The importance of patents and other mechanisms to enable inventors to capture some of the benefits of their innovations has long been recognized in the United States as a tool to encourage innovation, dating back to Article 1 of the U.S. Constitution and the 1790 patent law. Ensuring the protection of IP rights encourages the introduction of innovative products and creative works to the public. Protection is granted by guaranteeing proprietors limited exclusive rights to whatever economic reward the market may provide for their creations and products.

As we reported in April 2010, intellectual property is an important component of the U.S. economy, and the United States is an acknowledged global leader in the creation of intellectual property. According to the United States Trade Representative, "Americans are the world's leading innovators, and our ideas and intellectual property are a key ingredient to our competitiveness and prosperity." The United States has generally been very active in advocating strong IP protection and encouraging other nations to improve these systems for two key reasons. First, the U.S. has been the source of a large share of technological improvements for many years and, therefore, stands to lose if the associated IP rights are not respected in other nations. Secondly, a prominent economist noted that IP protection appears to be one of the factors that has helped to generate the enormous growth in the world economy and in the standard of living that has occurred in the last 150 years. This economist pointed out that the last two centuries have created an unprecedented surge in growth compared to prior periods. Among the factors attributed to creating the conditions for this explosion in economic growth are the rule of law, including property rights and the enforceability of contracts.[5]

[5]William J. Baumol, *The Free-Market Innovation Machine: Analyzing the Growth Miracle of Capitalism* (Princeton, N.J.: Princeton University Press, 2002).

The U.S. Economy May Experience Slower Growth Due to Lost Sales and Reduced Incentives to Innovate

The U.S. economy as a whole may grow at a slower pace than it otherwise would because of counterfeiting and piracy's effect on U.S. industries, government, and consumers. As we reported in April 2010, according to officials we interviewed and a 2008 OECD study,[6] to the extent that companies experience a loss of revenues or incentives to invest in research and development for new products, slower economic growth could occur. IP-related industries play an important role in the growth of the U.S. economy and contribute a significant percentage to the U.S. gross domestic product. IP-related industries also pay significantly higher wages than other industries and contribute to a higher standard of living in the United States. To the extent that counterfeiting and piracy reduce investments in research and development, these companies may hire fewer workers and may contribute less to U.S. economic growth, overall. The U.S. economy may also experience slower growth due to a decline in trade with countries where widespread counterfeiting hinders the activities of U.S. companies operating overseas.

The U.S. economy, as a whole, also may experience effects of losses by consumers and government. An economy's gross domestic product could be measured as either the total expenditures by households (consumers), or as the total wages paid by the private sector (industry). Hence, the effect of counterfeiting and piracy on industry would affect consumers by reducing their wages, which could reduce consumption of goods and services and the gross domestic product. Finally, the government is also affected by the reduction of economic activity, since fewer taxes are collected.

In addition to the U.S. economy-wide effects, as we reported in April 2010, counterfeit or pirated products that act as substitutes for genuine goods can have a wide range of negative effects on industries, according to experts we spoke with and literature we reviewed. These sources further noted that the economic effects vary widely among industries and among companies within an industry. The most commonly identified effect cited was lost sales, which leads to decreased revenues and/or market share.

[6]Organisation for Economic Cooperation and Development (OECD), *The Economic Impact of Counterfeiting and Piracy* (Paris: OECD, 2008).

Lost revenues can also occur when lower-priced counterfeit and pirated goods pressure producers or IP owners to reduce prices of genuine goods. In some industries, such as the audiovisual sector, marketing strategies must be adjusted to minimize the impact of counterfeiting on lost revenues. Movie studios that use time-related marketing strategies—introducing different formats of a movie after certain periods of time—have reduced the time periods or "windows" for each format as a countermeasure, reducing the overall revenue acquired in each window. Experts stated that companies may also experience losses due to the dilution of brand value or damage to reputation and public image, as counterfeiting and piracy may reduce consumers' confidence in the brand's quality.

Companies are affected in additional ways. For example, to avoid losing sales and liability issues, companies may increase spending on IP protection efforts. In addition, experts we spoke with stated that companies could experience a decline in innovation and production of new goods if counterfeiting leads to reductions in corporate investments in research and development. Another variation in the nature of the effects of counterfeiting and piracy is that some effects are experienced immediately, while others are more long-term, according to the OECD. The OECD's 2008 report cited loss of sales volume and lower prices as short-term effects, while the medium- and long-term effects include loss of brand value and reputation, lost investment, increased costs of countermeasures, potentially reduced scope of operations, and reduced innovation. Finally, one expert emphasized to us that the loss of IP rights is much more important than the loss of revenue. He stated that the danger for the United States is in the accelerated "learning effects"—companies learn how to produce and will improve upon patented goods. They will no longer need to illegally copy a given brand—they will create their own aftermarket product. He suggested that companies should work to ensure their competitive advantage in the future by inhibiting undesired knowledge transfer.

In addition, private sector organizations have experienced a wide range of incidents involving data loss or theft, economic loss, computer intrusions, and privacy breaches, underscoring the need for improved security

practices. The following examples from news media and other public sources illustrate types of cyber crimes.[7]

- In February 2011, media reports stated that computer hackers had broken into and stolen proprietary information worth millions of dollars from the networks of six U.S. and European energy companies.
- In mid-2009 a research chemist with DuPont Corporation reportedly downloaded proprietary information to a personal e-mail account and thumb drive with the intention of transferring this information to Peking University in China and also sought Chinese government funding to commercialize research related to the information he had stolen.
- Between 2008 and 2009, a chemist with Valspar Corporation reportedly used access to an internal computer network to download secret formulas for paints and coatings, reportedly intending to take this proprietary information to a new job with a paint company in Shanghai, China.
- In December 2006, a product engineer with Ford Motor Company reportedly copied approximately 4,000 Ford documents onto an external hard drive in order to acquire a job with a Chinese automotive company.

Quantifying Economic Impacts Is Difficult, However Industry Research Suggests the Impacts Are Sizable

Generally, as we reported in April 2010, the illicit nature of counterfeiting and piracy makes estimating the economic impact of IP infringements extremely difficult, so assumptions must be used to offset the lack of data. Efforts to estimate losses involve assumptions such as the rate at which consumers would substitute counterfeit for legitimate products, which can have enormous impacts on the resulting estimates. Because of the significant differences in types of counterfeited and pirated goods and industries involved, no single method can be used to develop estimates. Each method has limitations, and most experts observed that it is difficult, if not impossible, to quantify the economy-wide impacts. Nonetheless, research in specific industries suggests that the problem is sizeable.

[7]These examples are taken from GAO-12-876T.

Lack of Data Is the Primary Challenge for Quantifying Economic Impacts of Counterfeiting and Piracy

As we reported in April 2010, quantifying the economic impact of counterfeit and pirated goods on the U.S. economy is challenging primarily because of the lack of available data on the extent and value of counterfeit trade. Counterfeiting and piracy are illicit activities, which makes data on them inherently difficult to obtain. In discussing their own effort to develop a global estimate on the scale of counterfeit trade, OECD officials told us that obtaining reliable data is the most important and difficult part of any attempt to quantify the economic impact of counterfeiting and piracy. OECD's 2008 report stated that available information on the scope and magnitude of counterfeiting and piracy provides only a crude indication of how widespread they may be, and that neither governments nor industry were able to provide solid assessments of their respective situations. The report stated that one of the key problems is that data have not been systematically collected or evaluated and, in many cases, assessments "rely excessively on fragmentary and anecdotal information; where data are lacking, unsubstantiated opinions are often treated as facts."

Because of the lack of data on illicit trade, methods for calculating estimates of economic losses must involve certain assumptions, and the resulting economic loss estimates are highly sensitive to the assumptions used. Two experts told us that the selection and weighting of these assumptions and variables are critical to the results of counterfeit estimates, and the assumptions should, therefore, be identified and evaluated. Transparency in how these estimates are developed is essential for assessing the usefulness of an estimate. However, according to experts and government officials, industry associations do not always disclose their proprietary data sources and methods, making it difficult to verify their estimates. Industries collect this information to address counterfeiting problems associated with their products and may be reluctant to discuss instances of counterfeiting because consumers might lose confidence. OECD officials, for example, told us that one reason some industry representatives were hesitant to participate in their study was that they did not want information to be widely released about the scale of the counterfeiting problem in their sectors.

No Single Approach for Quantifying Impacts of Counterfeiting and Piracy Can be Used

As we reported in April 2010, there is no single methodology to collect and analyze data that can be applied across industries to estimate the effects of counterfeiting and piracy on the U.S. economy or industry sectors. The nature of data collection, the substitution rate, value of goods, and level of deception are not the same across industries. Due to these challenges and the lack of data, researchers have developed

different methodologies. In addition, some experts we interviewed noted the methodological and data challenges they face when the nature of the problem has changed substantially over time. Some commented that they have not updated earlier estimates or were required to change methodologies for these reasons.

A commonly used method to collect and analyze data, based on our literature review and interviews with experts, is the use of economic multipliers to estimate effects on the U.S. economy. Economic multipliers show how capital changes in one industry affect output and employment of associated industries. Commerce's Bureau of Economic Analysis guidelines make regional multipliers available through its Regional Input-Output Modeling System (RIMS II). These multipliers estimate the extent to which a one-time or sustained change in economic activity will be attributed to specific industries in a region.[8] Multipliers can provide an illustration of the possible "induced" effects from a one-time change in final demand. For example, if a new facility is to be created with a determined investment amount, one can estimate how many new jobs can be created, as well as the benefit to the region in terms of output (e.g., extra construction, manufacturing, supplies, and other products needed). It must be noted that RIMS II multipliers assume no job immigration or substitution effect. That is, if new jobs are created as a result of investing more capital, those jobs would not be filled by the labor force from another industry. Most of the experts we interviewed were reluctant to use economic multipliers to calculate losses from counterfeiting because this methodology was developed to look at a one-time change in output and employment. Nonetheless, the use of this methodology corroborates that the effect of counterfeiting and piracy goes beyond the infringed industry. For example, when pirated movies are sold, it damages not only the motion picture industry, but all other industries linked to those sales.

Economy-Wide Impact of Counterfeiting and Piracy Is Unknown

While experts and literature we reviewed in our April 2010 report provided different examples of effects on the U.S. economy, most observed that despite significant efforts, it is difficult, if not impossible, to quantify the net effect of counterfeiting and piracy on the economy as a whole. For

[8]Commerce, Bureau of Economic Analysis and Economics and Statistics Administration, *Regional Multipliers. A User Handbook for the Regional Input-Output Modeling System (RIMS II)*, 3rd ed. (Washington, D.C.: 1997).

example, according to the 2008 OECD study, it attempted to develop an estimate of the economic impact of counterfeiting and concluded that an acceptable overall estimate of counterfeit goods could not be developed. OECD further stated that information that can be obtained, such as data on enforcement and information developed through surveys, "has significant limitations, however, and falls far short of what is needed to develop a robust overall estimate." Nonetheless, the studies and experts we spoke with suggested that counterfeiting and piracy is a sizeable problem, which affects consumer behavior and firms' incentives to innovate.

Chairman Murphy, Ranking Member DeGette, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgement

If you or your staff have any questions about this testimony, please contact me at 202-512-3763 or offutts@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony include Christine Broderick, Assistant Director; Pedro Almoguera; Karen Deans; and Rachel Girshick.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper.

Mr. MURPHY. Let me start off by asking Mr. Lewis, if a U.S. company were to do these things to another U.S. company, hack into their computers, replicate projects, steal blueprints, et cetera, and basically make the same product, whatever it is, what kind of penalties would that U.S. company incur when they were caught, prosecuted?

Mr. LEWIS. There are several sets of penalties. The first is, of course, it could be liable to a lawsuit. We see lawsuits over IP violations frequently. Right? And if it can be proven in court, the damages can be substantial. Second, in some cases, the Economic Espionage Act can be applied to any company, U.S. or foreign, if they engage in this kind of activity. Third, there are computer security laws that if hacking occurs the company would be liable for that if it can be proven. One of the differences between the U.S. and countries like China and Russia is we have laws and we enforce them. They either don't have laws and they certainly don't enforce them. So in the U.S., you don't see as much of this if anything comparable at all.

Mr. GORTON. In other words, there are both criminal and civil penalties available in the United States.

Mr. MURPHY. But not ones that we can impose upon foreign nations when they do the same thing.

Let me follow up. Senator Gorton, and all of you, estimates show that the IP assets alone represent 75 to 80 percent of the S&P 500 market value, and the U.S. IP worth is at least $5 trillion, and licensing revenues for IP is estimated as 150 billion annually. So if cyber espionage is the biggest cyber threat America faces today, what really is at stake if we fail to act on it?

Mr. GORTON. I'm sorry. I missed the last part.

Mr. MURPHY. So if cyber espionage is the biggest cyber threat America faces today, what really is at stake if we fail to act on it?

Mr. GORTON. What's at stake is, first, others have testified to this, when it relates the our national defense, our very national security is at stake. When it can be measured by dollars, because that deals with civil, it is the $300 billion-plus losses that we found. And I must say, when we began this work, we found ourselves really sailing on uncharted seas. We didn't have a whole lot of earlier commissions that had worked on this. And our research was, to a certain extent, original.

Some people in the private sector didn't want to cooperate with us and were afraid of what would happen to them, sanctions that would be taken against them by China and the like. So I think that $300 billion-plus is a conservative estimate. The 2 million job loss comes from other sources. But between those two figures, that's what it's costing us.

Mr. MURPHY. And Dr. Wortzel, on that issue, too, and let me address this as well. What kind of protections are we missing here? And, of course, this also relates to the discussions taking place while Chinese delegation is in Washington today. But let's say, first of all, what kind of protections should we be dealing with in Congress? I know I read some things in your report. What would you add to that?

Mr. WORTZEL. China's goal in the dialogues right now is to limit all access to the Internet for domestic security. So I think we can

sort of leave them out of the equation. But I think the ability to link attribution and detection to criminal penalties, including arrest warrants, including limitations on travel, will really affect Chinese companies, Chinese leaders, and even individual actors. The Mandiant report identified, I think, four people by name showed who they are dating, showed what kind of car they drive. If that type of information was taken to a FISA court or some other court, an open court, and arrest warrants were issued, those people couldn't travel to the United States. And that would deter this.

Mr. MURPHY. Ms. Offutt, I have a question for you. So if you were advising the President and his staff this week as they are talking with the Chinese delegation in town what to push for, what would you say?

Ms. OFFUTT. The work that GAO has done on intellectual property also involves the evaluation of cyber threats and measures that can be taken in order to combat them. This is not an area as chief economist that I'm competent to talk about at length. But we have made recommendations about the adoption of measures at the firm level, for example, that involve people, processes, and software measures that can be taken to defend against any intrusions.

Mr. MURPHY. Thank you. I see my time is up, so I now go Ms. Schakowsky for 5 minutes.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. I just wanted to respond to comments that you made that the White House or the administration didn't decline—that declined to have any witness. Apparently, they suggested other administration witnesses than those who were unable because of scheduling reasons to come. And I just wanted to make that point.

Mr. Lewis, you wrote in your written testimony, "we need to recognize that many companies have not paid serious attention to securing their networks. There is no obvious incentive for them to do so."

How could that be?

Mr. LEWIS. There's not a lot of work on this. And what we know is probably about 80 to 90 percent of the successful cyber attacks against U.S. Companies only involve the most basic techniques. I used to look for Chinese super cyber warriors. They don't need super cyber warriors, they need a guy in a tee shirt who is going to overcome the truly feeble defenses. And some of it is companies don't want to spend the money. Some of it is——

Ms. SCHAKOWSKY. Aren't all the super cyber warriors just wearing tee shirts anyway?

Mr. LEWIS. We have pictures of some of them, which is aid in attribution issue. Sometimes companies spend money on the wrong stuff. And sometimes they don't want to know; it can affect their stock price, it may incur stockholder liability. So there's a whole set of incentives. It varies from sector to sector.

The banks do a tremendous job. And it's interesting to note that despite the fact that the banks do a tremendous job, they were largely overcome by Iranian cyber attacks over the last 6 months. Power companies, very uneven. There's three power companies in the Washington area. One does a great job, one does a terrible job. You know, it varies widely. We don't have a common standard. And there isn't a business model.

Now, this is beginning to change as CEOs realize the risk. But we are very far behind when it comes to corporate protection.

Ms. SCHAKOWSKY. Thank you. Dr. Wortzel, we—our government as a whole relies on—heavily on contractors. And that's especially true in the national security realm. Large projects rely on dozens of private sector contractors, layer upon layer of subcontractors, technology supply chains for military hardware are enormous. So how do we address the unique cyber security risks posed by long contracting and supply chains?

Mr. WORTZEL. Well, I think our supply chain has really big vulnerabilities. And the Commission has tried to look into this on major systems like the Osprey, the F–22, and a class of destroyers. And the Department of Defense could not go beyond the second tier in the supply chain. They don't know where this stuff is sourced from. So that's a huge problem.

The companies, in my opinion, that are in the defense industrial security program are getting good support from the Defense Security Service. They get regular visits. They get support from the Defense Security Service and the FBI on their cyber protections and their defenses. And it's not a perfect program, obviously, or we wouldn't have lost all that F–35 data. I think it's gotten a lot better. I think the FBI and the Department of Defense are—and the National Security Agency are doing a better job on intrusion monitoring for clear defense contractors.

Ms. SCHAKOWSKY. Let me ask you about the pipeline sector which has been considered vulnerable to cyber attacks. And anyone can answer that. Dr. Wortzel or Dr. Lewis.

Mr. WORTZEL. Well, our critical infrastructure, pipelines, are targeted by the Chinese military in case of a conflict. And those are private companies, run by private companies for the most part. And there simply is no legislation that would require those companies to maintain a set standard of security. And I think that's a huge vulnerability that has to be addressed.

Mr. LEWIS. You want to think about two sets of actors. The Chinese and the Russians have done their recognizance; they could launch attacks if we got in a war with them. But they're grown-up great powers. They are not going to just start a war for fun. On critical infrastructure, the greatest risk comes from Iran. Iran has significantly increased its capabilities, and they also are doing recognizance and targeting critical infrastructure, including pipelines. And so the Iranian Revolutionary Guard worries me more in this aspect than the PLA.

Ms. SCHAKOWSKY. Thank you. I yield back.

Mr. MURPHY. Thank you. Now recognize the vice chair of the full committee, Ms. Blackburn, for 5 minutes.

Mrs. BLACKBURN. Thank you all. And your testimony is absolutely fascinating. And I appreciate your time being here. I've got a couple of questions. Hope I can get through all of them.

Senator Gorton, I want to start with you. I appreciate so much what you said about having a major interest group in China that wants to join us in these efforts for IP protection and fighting the theft. I think that indigenous industry that feels as if they are worth being protected would be important. I appreciate that you have brought forward some recommendations. And I want to know

if you think there is anything that ought to be the first—the first salvo, if you will. What would be the very first step? Because we're in the tank on this. They've got a head start. This has become, as I said in my opening remarks, their economic development plan to reverse engineer and distill this IP theft. And we've got to put a stop to that. So item number 1, if you were to prioritize these recommendations, what should be first out of the gate for us?

Mr. GORTON. Thank you very much for that question. I was trying figure out how to answer it before you asked it. I think from the point of view of this committee, what might be the easiest and most appropriate first step would be to put one person, one office in charge. Our recommendation is that that be the Secretary of Commerce. That everything related to cyber security other than defense go through the Secretary of Commerce. That's where you'll begin to get control of those $300 billion and those 2 million jobs.

Even the response that you've received here today is there are all kinds of people in the administration, who is going to come and speak for them? There isn't one focal point. But if you make that focal point to the Secretary of Commerce, who does respond to you, I think it would be a major step forward.

Mrs. BLACKBURN. And I would imagine that you would recommend having that one person but with appropriate Congressional oversight and appropriate sunsets and all of that.

Mr. GORTON. Absolutely. And you are that oversight.

Ms. BLACKBURN. I appreciate that affirmation. So I thank you for that.

Mr. Wortzel, did you see The Washington Post this morning? The cover story, "Regimes Web Tools Made in the USA"?

Mr. WORTZEL. I did not.

Ms. BLACKBURN. I would just commend it to each of you to review. You're generous to give us your time this morning.

But let me ask you this, come to you with this question, since you're doing so much work in that U.S.-China relationship. And the problem there is significant. And we know that it bleeds over into Russia and then as you mentioned some of the other countries that are even less friendly to us.

So China has significant restrictions on the Internet and on Internet usage by the citizens and the population there. So if we were to establish rules of the road, if you will, for how we were going to respect the transfer of property, et cetera, over the Internet, how are we going to do this so that—with a country where our understanding of freedoms and our understanding of usage are so inherently and basically different.

Mr. WORTZEL. I don't think you can. My experience with China is they will steal and reverse engineer anything they can get their hands on. And I've been dealing with them full-time since about 1970. In the middle of their industries and delivering defense products to them. I think you really have to understand that the goal, and Jim outlined it nicely, the goal of Chinese Communist Party is to grow the economy, stay in power, and advance itself technologically. And most of the industries are state-owned or municipally-owned and directed by the government and aided by the intelligence services.

Mrs. BLACKBURN. Mr. Lewis, do you want to add anything to that?

Mr. LEWIS. Sure. I'm a little more positive. And I don't have Larry's long experience; I've only been negotiating with the Chinese since 1992. And we began negotiating with them on the issue of proliferation. And the Chinese used to be among the major proliferators in the world. And you can put together a package of measures that include sanctions, support from allies, direct negotiations with them. That can get them to change their behavior. So I'm confident that we can, if we keep a sustained effort in place, get them to act differently. And in part, it's because they know they're caught. They want to be a dynamic modern economy. You can't do that when you're dependent on stealing technology. They have a big contradiction. And we can sort of help them make the right decision.

Mrs. BLACKBURN. My time has expired. I have other questions, but I will submit those for the record.

Mr. MURPHY. I thank the gentlelady. I now recognize Dr. Burgess for 5 minutes.

Mr. BURGESS. Thank you, Mr. Chairman. And, yes, it is fascinating topic. I do have a number of questions, and I will have to submit, obviously, some of those for the record to be answered in writing.

But Dr. Wortzel and Mr. Lewis, when you heard my comments at the opening—yes, we're all concerned about sovereign spying and cyber security from a sovereign standpoint. Big businesses are concerned. Coca-Cola is smart not to put their formula on a network; that way, it's not available for theft. But what about the legions of small businesses out there? You had heard my comments in my opening statement. I'm concerned about the protection that they have or that they don't have from a liability perspective. So I guess, Mr. Lewis, my first question is to you. What—what can the small businesses do to improve their ability to prevent, identify, and mitigate the consequences of a successful compromise?

Mr. LEWIS. This is a major problem, because the small businesses are very often the most creative and the most innovative, and so we have to find ways to protect them. There's a couple of approaches that might be successful. NIST, as I think some of you said, is developing a cybersecurity framework. They are not allowed to use the word "standard," so they said framework, but if the framework comes out in a good place, it will lay out measures that any company can take to make their defenses better. We know how to do cybersecurity. We just don't have anybody really pushing that measure, and you can tell companies what to do. Hopefully NIST will do that.

The second one, and this relates to something that——

Mr. BURGESS. Let me stop you there and just ask you a question. Maybe you can tell companies what to do, so you are referring to Congress could legislate or mandate an activity that a company would have to do?

Mr. LEWIS. Let me give you an example which is, the people who are actually in the lead on this, in part because they enjoy so much attention from China, might be the Australians. So the Australian Department of Justice Attorney General, came up with a set of 35

strategies developed by their signals intelligence agency, and said, if you put these strategies in place, we will see a significant reduction in successful attacks. The Australians told me it was 85 percent reduction, and I said I don't believe it. So they let me go and talk to some of the ministries that tried it. They told me 85 is wrong; it is actually higher. That is now mandatory for government agencies in Australia. You can do this if you are a company. It is pretty basic stuff.

Mr. BURGESS. Now, are you at liberty to share that information with the committee so you could make that——

Mr. LEWIS. Oh, sure. I will definitely pass that along.

Mr. BURGESS. Thank you.

Mr. LEWIS. The second one, and this relates to I think something Larry said, is you can make the ISPs do a better job of protecting their customers. And they might want to do that for business reasons. Some of them already do, like AT&T or Verizon. But the ISP will see all of the traffic coming into the little company. They can take action before it reaches its target. So there's two things you could do that would make the world a better place.

Mr. BURGESS. And again, my comments during the opening statement, I'm concerned particularly for the small physician's office, the dentist's office, where there may be significant personal data put on a network as required now for electronic billing, and electronic prescribing that is now required of those offices. And yet, we provide no liability protection if one of those offices is hit with an attack.

It hasn't been a big story yet, but it is going to happen. We all know that it is going to happen. We had a dentist in Plano, Texas not too far away from the district that I represent, who lost a significant amount of personal data to some type of criminal attack in the cyberspace. I think we all know not to open the email from the Nigerian king who died and left you money in his will. But a lot of these attacks are sophisticated. Yes, it is small-potato stuff, but it's a lot of our businesses that can be affected.

Dr. Wortzel, do you have some thoughts about that?

Mr. WORTZEL. Mr. Burgess, I live in the first district of Virginia, Williamsburg, Mr. Whitman's district. Today in my district, the FBI is running a big seminar for all businesses and interested people on exactly this question. So the government is doing some things. I have to say that one of the positive areas of our dealings with China, is in bilateral cooperation on credit card and bank crime. So when it comes to the type of theft you are talking about, I think that between the Department of Treasury, and the FBI's legal attaches, you would see some progress.

Mr. BURGESS. Can I just ask you a question on that? Because that——

Mr. WORTZEL. Pardon me?

Mr. BURGESS. Can I ask you a question on that, because that does come up with some of our community banks. And they are sort of like the end user. They are the target organ, but really, it is the larger bank that deals with the offshore transaction that likely should have caught that activity, but it is always the smaller community bank that is then punished for having lost those funds for their—for their customer. So is there a way to actually involve

the larger offshore banks that are doing these offshore transactions?

Mr. WORTZEL. I'm afraid, I do not know the answer to that.

Mr. BURGESS. OK. If you can look into that and get back with us with some more information because that comes up all the time.

Mr. WORTZEL. I will do that. And I think the final thing I would say is, some of the equipment and programs that would protect small business are pretty expensive, $50,000 for a special monitoring router. But a group of businesses in an area could get together, share the cost of something like that, and mitigate these concerns.

Mr. BURGESS. Yes, if the Federal Trade Commission will let them. Thank you very much, Mr. Chairman.

Mr. MURPHY. The gentleman's time is expired. I now recognize the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. China plays a key role in cyber attacks against the United States. Of course, we have heard it recently because of some of our citizens going to China. Credible reports have noted that China has a government-sponsored strategy to steal American intellectual property in order to gain strategic advantage, and that Chinese military has been actively trying to steal military technology.

Dr. Wortzel, can you explain why China is, far and away, the number one perpetrator of these attacks and what is the history here and how long has this been going on?

Mr. WORTZEL. Well, the first really open documentation of it, Mr. Green, was the report, three series of reports by TIME Magazine, the Titan Rain penetrations. Now, the poor guy that went to the government and said this is going on, and pinpointed it to China, got frustrated because there wasn't a government response. He leaked it to TIME Magazine, he lost his security clearance and his job. So the government has got to acknowledge that this is happening.

Mr. GREEN. Yes.

Mr. WORTZEL. And it really owes it to the citizens to do this. But I think it is important to understand that the third department, the signals intelligence department of the People's Liberation Army and the fourth department, the electronic warfare and electronic countermeasures department work together. The third department alone has 12 operational bureaus looking at strategic cyber, and signals, three research institutes, four operational center, and 16 brigades with operational forces. And that about half that number that—are the people that do the door kicking and penetrate in the fourth department. That leaves out the Ministry of State Security. That leaves out 54 state-controlled science and technology parks, each of which are given specific strategic goals by the Chinese government, and Chinese Communist Party to develop different technologies. So we just face a huge threat. And that's why I'm a little more pessimistic than Jim in solving it.

Mr. GREEN. Mr. Lewis, do you have anything to add to that?

Mr. LEWIS. The Chinese economic espionage began in the late 1970s with opening to the west. It has been part of their economic planning since then. What happened at the end of the 1990s, was that the Chinese discovered the Internet, discovered it is a lot easi-

er to hack than to cart off a whole machine tool or something. And so this has been going on for over 30 years. It is a normal policy for them. I'm a little more optimistic though. You can get them to change if you put the right set of pressure and pressure points on them.

Mr. WORTZEL. I will give you two examples, if I may. I delivered as the Assistant Army Attache, a U.S. Army artillery-locating radar to the Chinese military. And I noticed that I began to get orders, or requests for resupply of certain parts. And the radars were supposed to be down on the Vietnam border. So I went to the Thai Army, the U.S. attache in Thailand and said, hey, are these parts failing in your equipment, same rough environmental problem? And they had a zero failure rate. So within 4 months, they had reverse engineered these radars, and what they couldn't build, they kept saying they had part failures so they would get parts and try and reverse engineer those.

Another time after the Tiananmen massacre in '89, another attache and I were out in Shandong Province and we had a down day, and we asked to visit a PLA, People's Liberation Army radio factory. And sure, they said come in. Things were still in pretty good shape between the U.S. military and the Chinese, and they showed us their research and development shop for new radios and cell phones. And they were literally disassembling and copying Nokia cell phones, and Japanese radios. So it is a long tradition there. It goes back to 1858 and the self-strengthening movement when they went out, bought and copied the best weapons and naval propulsion systems in the world. Of course, they got beaten by the Japanese in 1895, and that put an end to that.

Mr. GREEN. Well, the Chinese government officially denies they conduct cyber espionage, and what evidence is there that the country is behind many of these attacks outside of your vigil there at the PLA?

Mr. WORTZEL. Well, I think the Mandiant Report did an excellent job. I think that the director of the National Security Agency, and the National Counterintelligence Executive have provided a great deal of evidence on attribution, as has the FBI.

Mr. LEWIS. There is a classified report put out by the Director of National Intelligence that probably has not been made available to the committee. You might want to ask for it.

Mr. GREEN. OK.

Mr. LEWIS. I will give you an example from these talks we had with the Chinese. We spend an entire day talking about economic espionage. And at the end of it—including the Economic Espionage Act. At the end of it, a PLA senior colonel said to us, look, in the U.S. military espionage is heroic and economic espionage is a crime, but in China, the line is not so clear. So one of the things we can do is make the line a little clearer to them.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. MURPHY. The gentleman yields back. The chair will now recognize Mr. Johnson from Ohio for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman, and I appreciate so much the opportunity to hear from the panel today. I spent nearly 30 years in information technology in the Air Force and in the private sector before coming to Congress. And I know that this is a

tremendously complex and concerning issue because computing technology, at its very base, is not that complicated. It's ones and zeros. And for malicious nations like China and others who understand how to manipulate ones and zeros, this is not going to be an issue that we can solve today and then put it on the shelf and come back and look at it 5 years from now, and upgrade it and that kind of thing. This is going to be a daily, daily obligation to protect not only our national security, but our industries, and our businesses across the country.

So I'd like to ask just a—just a few questions. Dr. Lewis, in your testimony, you stated that it would be easier for China to give up commercial espionage if the cost of penetrating business networks is increased and the return from those penetrations are minimized. How, given the ease with which this can be done by computer practitioners, how can we increase the cost to China that will dissuade them?

Mr. LEWIS. We can make it a little harder for them, and since you are familiar with the information technology, and probably all of you have done this with consumer goods, when you buy something, the user name is "admin," and the password is "password." And what we found repeatedly through research at both government agencies and corporations, is that people forget to change, right, so they leave the password as "password." And you know what, it doesn't take a mastermind to hack into a system if the password is "password." There are other things you can do.

You can restrict the number of people who have administrator privileges. If you look at Snowden for example, he had administrator privileges and that let him tromp all around the networks he was responsible for and collect information. You shouldn't let that happen. You can make passwords a little more complex. If passwords are your dog's name, or any of your first cars, or something like that, the people who do this for a living can usually guess that in under 2 minutes. Right, it is not——

Mr. JOHNSON. There are algorithms out there that will figure out passwords, so I'm not sure password security is going to solve the problems of a nation state like China.

Mr. LEWIS. And that's why we need to move away from passwords, and I hope that the NIST standards recognize that passwords failed more than a decade ago; we need to do something else. There are a number of small steps that can make it harder. Right now it is so easy to get into most networks that there is really little cost for the hacker. He doesn't have to put a lot of effort in.

Mr. JOHNSON. Sure, Senator Gorton, I was positively intrigued by your comment that there needs to be one agency, or one person in charge. And I really believe that that has merit. I'm not sure who it should be. I haven't given that a whole lot of thought, but I certainly agree that there needs to be someone at the cabinet level that is responsible and accountable for overseeing this effort.

Your report outlines a number of policy solutions that aim to address the loss of our intellectual property and technology. So kind of continuing along the lines of what you said earlier, is the government properly equipped to enforce the IP rights against foreign companies and countries, or are we too fractionalized to properly deal with the issue? And I submit, and you know, I admit full up,

you know, even—even CEOs of companies today, their eyes glaze over when you start talking about information technology in its core application, because it's a complex environment.

Do we have the right people? Do we have the right skill sets? Do we have the right focus to try and address this?

Mr. GORTON. Well, we are decentralized, and I think it is very important that we—that we do create responsibility at, you know, at one place to the maximum possible extent. I would add to Mr. Lewis's,one of the recommendations we make, is to make it easier to seize goods that violate—that have violations of intellectual property when they arrive in the United States. A few years ago, we made it somewhat easier to go to court and to get seizures. It's nowhere near easy enough. And one of our principal recommendations is to allow on any kind of probable cause the temporary seizure of those goods when they arrive, and then get to court, and deal with it afterwards. So to a certain extent, it is a lack of decentralization. To a certain extent it does require tougher laws.

Mr. JOHNSON. Yes. Well, my time is expired. I had much more I wanted to talk about, but maybe we will get to that another time. Thank you, Mr. Chairman, I yield back.

Mr. MURPHY. The gentleman yields back. The chair will now recognize Mr. Tonko from New York for 5 minutes.

Mr. TONKO. Thank you, Mr. Chair. Ms. Offutt, do you agree with the IP Commission's assessment of the value of the loss of intellectual property?

Ms. OFFUTT. The work that we did suggests that an estimate like that, that's based on the application of a rule of thumb about the proportion of an industry's output that is vulnerable to or lost to intellectual property theft, is not reliable. There's certainly no way to look across all of the diverse sectors of the economy and suggest that the theft is characterized in any particular way that would be common to all of them.

So the estimate that has gained currency, certainly in discussions, is, in our view, not credible. It's based on first, the notion that one-third of the economy's output comes from intellectual property-intensive industries. That means, essentially, companies that have a lot of patents, trademarks, copyrighting, that probably tells you what is at risk. But the application of the rule of thumb, which is 6 percent of that output being lost, we don't find any basis for believing that to be an accurate number.

Mr. TONKO. Thank you, and while I understand the cost of IP theft is difficult to quantify, it has been suggested that the theft costs us over $300 billion annually in losses to the U.S. economy. I would like to try to further distinguish the types of IP theft. The Mandiant Report from February traced Chinese government support for cyberattacks. The Defense Department's 2013 report to Congress on China explicitly mentions Russia's concerns about IP protection and how they will affect the types of advanced arms and technologies it is willing to transfer to China. So clearly, even Russia is concerned about Chinese state-sponsored IP theft. Can any of you as witnesses discuss the extent of state-sponsored IP theft?

Mr. LEWIS. In China, or globally?

Mr. TONKO. Globally, or if you want to do both, that would be fine.

Mr. LEWIS. Both Russia and China have very tight control, very tight links to—between the government, and the hackers. I think that China is more decentralized, and one of the problems they will have in getting it under control is that, you know, regional PLA organizations, regional political organizations engage in independent action, right, not necessarily alerting Beijing to what they are doing. So it is a more decentralized system, and I think that the Chinese will have difficulty controlling it.

In contrast, Russia is—appears to be very tightly centralized. All activities are controlled by the FSB. The Russians have a tremendous domestic surveillance capability, it is called SORM, SORM–2, in fact, that allows them to know what everyone is doing on the Internet. And so if you are a hacker and you are playing ball in Russia, you have to go along with what the FSB wants you to do.

Mr. TONKO. Anyone else on that topic?

Mr. WORTZEL. Well, I think it's important to understand that in China, if they want to track down five religious people praying in a house church with unauthorized Bibles, they can do it. It's a pretty security-intrusive place. And if they wanted to track—if somebody gets on the Internet and is engaging in a form of political protest, they will get them and they will be in jail. So they can do what they want to do. They have that capacity. It's just that the state policy is, get this technology, so they don't bother with them.

I would also like to suggest, if I may, that there are ways we can make things harder. I mean, you can—you can encode a digital signal in a file and attach that as you would a patent, copyright, or trademark, and a company that's developing a technology could do that, and then if you find that technology—if you find that code appearing elsewhere in China's, or Russia's control technologies, you could take legal action just as you would for a patent, copyright, or trademark. I am not quite sure that our intellectual property laws are up to that yet, but could you do that.

Mr. TONKO. Just quickly when you look at the state-supported effort for IP theft, and contrast that with individuals in criminal networks, what do you think the percentage breakdown would be if you had to guess at it?

Mr. LEWIS. In Russia, and China, I don't think there are any independent actors. I think that the degree of control that the government agencies exercise is—it is not like they are telling them this is what you have to do, but the criminals are appendages of the state, or they are tolerated by the state and in some cases they are directed by the state. So it is a different system over there, and I think that the degree of independent action is very, very limited.

Mr. GORTON. In India you might find a good deal of independent action.

Mr. TONKO. OK, thank you, Senator. With that I yield back, Mr. Chair.

Mr. MURPHY. The gentleman yield back. I will now recognize myself for 5 minutes of questions, and Senator Gorton, I would like to follow up on your idea of what would be best if you had one person who was responsible for overseeing all this. And I know that others have discussed that, and I would also like to ask you if you know that Victoria Espinel is the U.S. Intellectual Property Enforcement Coordinator approved by the U.S. Senate in 2009 in

charge of the Obama administration's overall strategy for enforcement of intellectual property rights. Is that someone that you think would be helpful? She was invited and declined our invitation to attend today, but is that what you and Mr. Lewis, and others have in mind?

Mr. GORTON. I would like to know what she would have said.

Mr. MURPHY. Same here. If I could ask you, Senator, as we look around the world and see what is going on, what we are having to combat here, do any other countries stand out as one that is perhaps doing it right, doing a significantly appropriate job on this?

Mr. GORTON. I don't think so, but that wasn't something that was a central point of our investigation.

Mr. MURPHY. OK.

Mr. GORTON. We were interested in what we did here. And Mr. Chairman, may I apologize? I didn't realize it would last so long. I have a noon date over on the Senate side that I'm going to have to leave now.

Mr. MURPHY. And we thank you for your time, and we certainly excuse you in light of that.

Mr. GORTON. And I thank you. This is a vitally important mission on your part. And to take real action to protect our intellectual property will be a great service to the country.

Mr. MURPHY. And if anyone has any additional questions after your departure, we will see that they are submitted to you in writing. Thank you very much, Senator, for your time.

All right, if I may ask you, Dr. Lewis. In your testimony, you said that it would be easier for China to give up commercial espionage as the cost of penetrating business networks is increased, and the returns from those penetrations are minimized. And I know we discussed that some, but would you give us some examples, or how you think we can increase the cost to China from commercial espionage?

Mr. LEWIS. Sure, and just to briefly respond to your question to Senator Gorton, the U.K., France, and Russia all have pretty effective programs in place. They are not watertight, but they are further along than we are. And some of it is different constitutional arrangements. The Australians have made some progress. If it's any consolation, people who are doing a worse job than us are the Chinese. They are in terrible shape when it comes to defense, and they remind me of that all the time. I think what we need to do, it is not enough of a consolation, but it is better than nothing, right? We need to find ways to get companies to harden their networks. And that involves identifying practices that would make the networks more difficult to penetrate and control. There are an identified set of practices. Hopefully NIST will encapsulate them. We need to think about better ways to share threat information. I know CISPA has attracted mixed review, the Cybersecurity Information Sharing Protection Act. We need some vehicle to let companies and government share information better on threats. That can be relatively effective.

Finally, I'm a little surprised to hear commerce held up as the place you would want to coordinate. We do have a policy coordinator in the White House. She is doing a pretty good job. But the place where we have not done enough as a Nation is thinking

about the role of the Department of Defense, and defending our network. And it is a bit of a sensitive topic at this time. You know, it's not the exact moment to come up and say we should give NSA a little more responsibility, but they do have capabilities that we are not taking full advantage of.

Mr. MURPHY. At this time, I will yield back and recognize the gentleman from Texas, Mr. Olson, for 5 minutes of questions.

Mr. OLSON. Thank you, Mr. Chairman, and I want to thank the witnesses for being here this morning. Senator Gorton left, so I can't talk about being through Evansville, Indiana. But, Mr. Lewis, I have been in Pittsburgh, and I have seen a great side of injustice and theft. As you know, I'm talking about the 1980 AFC championship game in which Mike Renfro from the Houston Oilers scored a touchdown that the refs disallowed. But turning to other thefts, as we heard from all of you, state-sponsored terrorism, cyber espionage, is having a devastating effect on the American economy and the competitiveness of American companies. And the energy industry, important in my home state of Texas, is particularly vulnerable to cyberattacks. These attacks come in two forms, as you all know. One type is where a malicious actor could disrupt the physical operations by hacking into the industrial control systems which are used to control everything from the power grids to pipelines. The other cybersecurity threat to the energy industry, which is what this hearing is focused on, is the theft of intellectual property and proprietary information through cyber espionage. And the most malicious of these hackers are nation states, North Korea, Iran, Russia, and China.

My question will focus on China this morning. Over the past couple of years, there have been several news reports of major American oil and gas companies being targeted by Chinese hackers. And yes, despite official denials we have been able to trace these attacks back to China. And some of these companies are headquartered in my hometown of Houston, Texas. The hackers are looking for, as you all know, sensitive information, such as long-term strategic plans, geological data showing locations of oil and gas reserves; even information on the bids for new drilling acreage.

This type of information is worth billions of dollars, Senator Gorton's committee, $300 billion in lost revenue for Americans. This disclosure can severely hurt a company's competitiveness. My first question for you, Dr. Wortzel, would you say that energy is a strategic industry in the eyes of the Chinese government?

Mr. WORTZEL. It is absolutely a strategic industry, and they gather that business intelligence, the state does, for a couple of reasons. First of all, they are looking for technology because in some areas they are behind. Second, they are beginning to invest here. So they want to know where to invest. They want to know where they are going to get the most money for their investment, and where they can extract the most technology.

Now, with respect—I think it is also important to remember that any time a critical, or a control system is penetrated, or a computer system is penetrated, it is also mapped. So it's only in terms—in time of conflict that that penetration may be used for a critical in-

frastructure attack because that would be an act of war. But the damage is done, and they know what to do.

Mr. OLSON. Yes, sir, and I know they have invested billions of dollars in the Eagle Ford shale play with American partners, and I suspect they are trying to get that technology, some of the drill bit technology, other things, hydraulic fracturing because they have shale plays in Western China. It's a very difficult terrain out there, different, you know, different geological structures, but it is pretty clear to me that they are involved with us trying to steal our technology as opposed to being good corporate partners.

And my final question is for you, Mr. Lewis. We will put aside the 1980 AFC championship game, but how is the industry working together with government to combat cyber espionage?

Mr. LEWIS. This is one of the harder areas, and so people have been trying since 2000 to come up with a good model for what they call public-private partnership. And it looks like it has to vary from sector to sector. So for example, the banks, the telcos, they have a pretty good partnership with the government. Other sectors maybe the electrical sector, a little less strong partnership.

So one of the things we need to do is maybe take a step back and say, what are the things that would let companies feel comfortable working with the government? What are the things that would let them feel comfortable sharing information or getting advice. And there has been some effort to do that, but we haven't done enough, and what we haven't done in particular is tailor it to each sector. What the concerns of an oil company are, are going to be different from the concerns of a software company. So maybe a new approach, focused a little bit more on sector-specific ideas.

Mr. OLSON. No one-size-fits-all, and I am out of time. I yield back. Thank you, sir.

Mr. MURPHY. The gentleman's time is expired. I now recognize the gentleman from Louisiana, Mr. Scalise, for 5 minutes.

Mr. SCALISE. Thank you, Mr. Chairman. I appreciate you holding this hearing, and appreciate our panelists for participating. I know our committee has delved into this on a number of different fronts. There has been a lot of attempts over the last few years to try to move legislation through Congress to address this in different ways. And it's a serious problem. I know a few of you have pointed out the economic impact. There have been a lot of independent studies. Of course, the IP Commission report that Senator Gorton was part of, and really helped lead, estimates a $300 billion a year lost in our economy, and over 2 million jobs.

And when you go out to places like Silicon Valley, which, you know, for the tough economic times we have right now, there are a lot of industries that are struggling, but one of the few areas that is a bright spot is the technology industry. And in large part, because so much of that intellectual property starts, is created, and has been innovated here in the United States, and it's being stolen. It is being stolen by countries like China. And we know about it. We sometimes can stop it, and often can't. And yet, it has a major impact on the economy, but it's kind of lost in the shadows because it is not always quantifiable.

I want to ask you, Ms. Offutt. You talked a little bit about this. Is there a better way to gather data, a better way to know if that

$300 billion number per year, is right? Is it way too low? You know, what are—is there a better way to find out just what is being stolen, and how it impacts our economy?

Ms. OFFUTT. Well, I think the approach is necessarily at the sector or the firm level. That's the way we would aggregate to a number that told us something meaningful about the extent of what is at risk, what has been compromised, and then how it has been used to affect firm sales or consumer purchases. And that effort is quite data- and labor-intensive, but some of those data may become available as we intensify efforts to actually impose protection. Although it would probably always be the case that firms will be reluctant to divulge everything about compromise of their systems, for competitive reasons primarily.

Mr. SCALISE. Do you think the criminal enforcement is adequate? Do you think our Federal agencies that are tasked with enforcing these laws, are they doing enough? Does more need to be done? Is it that the law doesn't give them the kind of ability they need to go after the actors that are out there stealing all of this property? Anybody on the panel.

Ms. OFFUTT. I defer to Mr. Lewis to answer that question.

Mr. SCALISE. Mr. Lewis, you can——

Mr. LEWIS. Let me give you an example that was startling, even to me. I was at a meeting recently with some FBI representatives from a major city, not in a State from any of you, I'm happy to say. They told me they won't take a case of cyber crime if the loss was less than $100 million.

Mr. SCALISE. What agency said this?

Mr. LEWIS. FBI.

Mr. SCALISE. Why is that?

Mr. LEWIS. Because there's just so many that they can't do them all, and so we have a real problem here. The issue is not in the United States. If you commit a crime through hacking in the United States, you will go to jail. The FBI is tremendously effective. If you commit a crime in Western Europe, or in Japan, or Australia, you will go to jail. The countries that observe the law do a good job. And so what we have seen is the hackers have moved, or the ones who have survived, live in countries that either support this, or don't have the good rule of law.

So Brazil, Nigeria, you know about them, Russia, and China, they encourage them. That's our fundamental problem is if we could let the FBI off the leash, if they could get cooperation from these countries, this problem would be much more manageable. But you have places that don't find it interesting to cooperate.

Mr. SCALISE. And I will stick with you on this one, Dr. Lewis. We do hear from companies that say that there is a reluctance to share information with the Federal Government, you know, in some cases where that information can be helpful in at the deterring this theft, or kind of better protecting against it. What do you see as maybe an impediment, or what things can be done to better improve that ability to hopefully lead to a better process that stops some of the stuff from occurring in the first place?

Mr. LEWIS. That's one of the subjects of debate now, but you probably need better liability protection for the companies, and you probably need some guarantee that if you give information to the

government, it won't go to every agency under the sun. You need some sort of limitation on it. Those are the two key areas there. Antitrust comes up as a problem as well if companies share information, they might run afoul of antitrust. So liability, antitrust, and data security are the three obstacles.

Mr. SCALISE. And I know those things—are things we are struggling with here, too. So I appreciate that. Thank you, Mr. Chairman. I yield back the balance of my time.

Mr. MURPHY. I thank the gentleman for yielding back. I also thank all of our panelists, and thank the members. What we have heard today is startling and enlightening on this issue that would have a huge impact upon our national security, but also our jobs, and at a time where we all want to see more Americans going to work, it is sad that this state of affairs exists, but we thank the information the panelists have given us today.

I also want to ask for unanimous consent to enter into the record a letter from the Cybersecure America Coalition on today's hearing. I understand the minority has had a chance to review this letter and does not object, so hearing no objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. MURPHY. And I ask unanimous consent that the written opening statements of other members be introduced into the record. So without objection, the documents will be entered into the record. So in conclusion again, I thank the witnesses and members who participated at today's hearing. I remind Members that they have 10 business days to submit questions for the record, and I ask the witnesses all agree to respond to the questions. That concludes our hearing today, thank you.

[Whereupon, at 11:52 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

The Honorable Tim Murphy
Chair, Subcommittee on Oversight and Investigations
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

July 9, 2013

Dear Chairman Murphy:

I am writing to commend you for your leadership on the issue of cyber security and to thank you for holding the July 9th hearing entitled: Cyber Espionage and the Theft of U.S. Intellectual Property and Technology. This is a critical issue for our nation which requires strong leadership from Congress if we are able combat this threat.

I write today as Executive Director of the Cyber Secure America Coalition, a collection of companies dedicated to pursuing positive cyber security legislation necessary to make the U.S. IT infrastructure more secure. Our Coalition members are leaders in the industry and include, Kaspersky Lab, TrendMicro, Qualys, CyberPoint, TechGuard Security and Nok Nok Labs. Combined these companies represent decades of efforts to fight cyber threats including cyber espionage and the theft of intellectual property, so critical to the competitive advantage we need in this country to innovate and promote our nation's economic well being.

In today's cyber world, the threats are real, sophisticated and coming at a more rapid pace. Gone are the days when viruses were just a form of graffiti on the Web. Today, cyber criminals in all forms are focused on stealing valuable information, whether it is credit card numbers, personal data, corporate information or classified government information. It is a much more dangerous world in cyber space. We believe that this will only continue to escalate as more and more valuable information is available in digital form.

It is easier to hide one's identity or location in the cyber world versus the physical world. Thus it becomes relatively more difficult in the cyber world to catch those that would do harm. The record shows, however, that it is possible through cooperation and effort of law enforcement at all levels, including at the international level with organizations like Interpol to catch cyber criminals. It is also clear that we need appropriate cyber crime penalties to punish those that

are apprehended. We believe that governments must send the message that cyber crime does not pay.

To effectively combat cyber espionage and intellectual property theft, the Cyber Secure America Coalition believes that there are key legislative actions that can help to protect against the cyber threats of today and beyond. It is critical that key U.S. business and government entities take steps to strengthen individual and collective cyber security and protect critical digital assets. Therefore we recommend the following actions:

1. Passage of enhanced information sharing legislation about cyber threats between the private sector and the federal government to improve cyber security. This will provide real-time actionable intelligence that will help better protect against cyber attacks. Legislation must include liability protection from lawsuits for those that share information in good faith for the purpose of improving cyber security.

2. Safe Harbors from disclosure of cyber attacks should be developed to support companies that meet certain security frameworks as an to incentive to improve baseline security. To achieve a safe harbor, companies should at least take steps along the lines of the following:

- Demonstrate continuous monitoring of enterprise security architecture through a cyber security "industry standard" regime. An example would be the "SANS 20 Critical Controls" that are widely deployed by companies that are serious about security;

- Demonstrate compliance with all relevant federal and state cyber security laws such as data breach notification and HIPAA; and

- Designate an officer of the company with responsibility and accountability for cyber security.

3. Identification of the most important aspects of the critical infrastructure and steps should be taken to better protect the integrity of those systems. This includes the development of voluntary, flexible standards for the critical infrastructure. These standards should be based on existing international standards and best practices. There should be incentives for implementation, and liability relief for those critical infrastructure industries that participate in such a voluntary program.

The Cyber Secure America Coalition is committed to being a partner in helping to better secure our national digital assets. We need to do more to combat cyber espionage and intellectual property threat. Improved cyber security in the public and private sectors can achieve that objective. No security is perfect, but we must do more to ensure that our competitive advantage remains. The US competitive advantage in e-commerce and innovation is, in the view of our member companies, critical to restoring and enabling vibrant economic growth. We look forward to working with the Subcommittee as you tackle this important issue in the months ahead.

Thank you again for your leadership.

Sincerely,

Phil Bond
Executive Director

The Honorable Diana DeGette
Ranking Member, Subcommittee on Oversight and Investigations
House Committee on Energy and Commerce
2322A Rayburn House Office Building
Washington, DC 20515

July 9, 2013

Dear Ranking Member DeGette:

I am writing to commend you for your leadership on the issue of cyber security and to thank you for holding the July 9th hearing entitled: Cyber Espionage and the Theft of U.S. Intellectual Property and Technology. This is a critical issue for our nation which requires strong leadership from Congress to combat this threat.

I write today as Executive Director of the Cyber Secure America Coalition, a collection of companies dedicated to pursuing positive cyber security legislation necessary to make the U.S. IT infrastructure more secure. Our Coalition members are leaders in the industry and include, Kaspersky Lab, TrendMicro, Qualys, CyberPoint, TechGuard Security and Nok Nok Labs. Combined these companies represent decades of efforts to fight cyber threats including cyber espionage and the theft of intellectual property, so critical to the competitive advantage we need in this country to innovate and promote our nation's economic well being.

In today's cyber world, the threats are real, sophisticated and coming at a more rapid pace. Gone are the days when viruses were just a form of graffiti on the Web. Today, cyber criminals in all forms are focused on stealing valuable information, whether it is credit card numbers, personal data, corporate information or classified government information. It is a much more dangerous world in cyber space. We believe that this will only continue to escalate as more and more valuable information is available in digital form.

It is easier to hide one's identity or location in the cyber world versus the physical world. Thus it becomes relatively more difficult in the cyber world to catch those that would do harm. The record shows, however, that it is possible through cooperation and effort of law enforcement at all levels, including at the international level with organizations like Interpol to catch cyber criminals. It is also clear that we need appropriate cyber crime penalties to punish those that

are apprehended. We believe that governments must send the message that cyber crime does not pay.

To effectively combat cyber espionage and intellectual property theft, the Cyber Secure America Coalition believes that there are key legislative actions that can help to protect against the cyber threats of today and beyond. It is critical that key U.S. business and government entities take steps to strengthen individual and collective cyber security and protect critical digital assets. Therefore we recommend the following actions:

1. Passage of enhanced information sharing legislation about cyber threats between the private sector and the federal government to improve cyber security. This will provide real-time actionable intelligence that will help better protect against cyber attacks. Legislation must include liability protection from lawsuits for those that share information in good faith for the purpose of improving cyber security.

2. Safe Harbors from disclosure of cyber attacks should be developed to support companies that meet certain security frameworks as an to incentive to improve baseline security. To achieve a safe harbor, companies should at least take steps along the lines of the following:

- Demonstrate continuous monitoring of enterprise security architecture through a cyber security "industry standard" regime. An example would be the "SANS 20 Critical Controls" that are widely deployed by companies that are serious about security;

- Demonstrate compliance with all relevant federal and state cyber security laws such as data breach notification and HIPAA; and

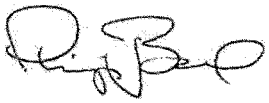
- Designate an officer of the company with responsibility and accountability for cyber security.

3. Identification of the most important aspects of the critical infrastructure and steps should be taken to better protect the integrity of those systems. This includes the development of voluntary, flexible standards for the critical infrastructure. These standards should be based on existing international standards and best practices. There should be incentives for implementation, and liability relief for those critical infrastructure industries that participate in such a voluntary program.

The Cyber Secure America Coalition is committed to being a partner in helping to better secure our national digital assets. We need to do more to combat cyber espionage and intellectual property threat. Improved cyber security in the public and private sectors can achieve that objective. No security is perfect, but we must do more to ensure that our competitive advantage remains. The US competitive advantage in e-commerce and innovation is, in the view of our member companies, critical to restoring and enabling vibrant economic growth. We look forward to working with the Subcommittee as you tackle this important issue in the months ahead.

Thank you again for your leadership.

Sincerely,



Phil Bond
Executive Director

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

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

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

Attachment

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.

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

Dr. Larry Wortzel
Commissioner
U.S.-China Economic and Security Review Commission
444 North Capitol Street, N.W., Suite 602
Washington, D.C. 20001

Dear Dr. Wortzel:

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

Hall of The States, Suite 602
444 North Capitol Street, N.W.
Washington, D.C. 20001

Phone: 202.624.1407
Fax: 202.624.1406
E-mail: contact@uscc.gov
www.uscc.gov

U.S.–China Economic & Security Review Commission

William A. Reinsch, Chairman
Dennis C. Shea, Vice Chairman

Representative Tim Murphy
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6371

Dear Chairman Murphy,

I am pleased to respond to questions posed by Members of the House Energy and Commerce Oversight and Investigations Subcommittee regarding my testimony provided on July 9, 2013. These responses represent my own views and not those of the U.S.-China Economic and Security Review Commission.

Additional Questions for the Record

The Honorable Tim Murphy

1. **There has been tremendous attention recently by the Administration on this issue of cyber espionage. Statements by Secretary Lew, General Keith Alexander, and the President himself. Are they having any impact?**

   It is useful to raise public, government and corporate awareness of the threat of cyber espionage; therefore I think statements by officials such as Secretary Lew and General Alexander have some impact.

   a. **Has cyber espionage supplanted terrorism as the number one threat to this country as some in the Administration have suggested?**

      Cyber espionage costs the United States a lot of money and, in part, may be linked to network reconnaissance that later can be used in war or for cyber terrorism. However, the threat of traditional terrorism, in my view, remains high. Also, cyber espionage does not directly kill people or destroy property, while terrorism can be deadly.

2. **We hear from companies constantly that they do not want to share information about their incidents out of either fear or shame that something bad has occurred. They are especially reluctant to share an incident if it means they lose sensitive IP or technology. Is this a good approach for companies? What do they have to gain by not reporting this information?**

In the long run, companies might do better if they came to some common agreement to disclose incidents. However, I am sure that individual corporate counsel and boards will set policies that they believe are best for the corporations. By not reporting information, companies do not face a potential loss of consumer confidence, lower public opinion about the brand, or a potential loss of stock value.

a. **Are U.S. companies fearful that if they report this type of information they will lose market share or future business in China?**

In meetings in China with US companies and with officers of the American Chamber of Commerce, commissioners have been told privately by many corporate representatives that one reason they hesitate to complain about Chinese cyber activity and about intellectual property theft is that they fear that the Chinese government will retaliate against the company.

3. **What is our biggest leverage against the Chinese for their acts of cyber espionage?**

The biggest leverage we have against any country for acts of cyber espionage is to prosecute perpetrators for criminal activity and to sanction governments, individuals and companies that engage in intellectual property theft.

a. **What role do companies have in protecting themselves?**

Companies are responsible for their own protection. If companies are part of a government program, like the defense industrial security program, the government can and should set standards for protecting information. As I said in my testimony at the hearing, however, when the aggregate of economic damage from cyber espionage is as great as we see, I think President Obama can use the powers he has under the International Economic Emergency Powers Enhancement Act to sanction companies, individuals and countries that engage in this cyber espionage.

b. **Are other countries raising the issue of cyber espionage with China through diplomatic channels?**

Australia, Germany, Canada, the United Kingdom, and India, according to their own press, have raised the issue with China in diplomatic channels.

4. **Can you explain how information or data obtained through cyber espionage is used to reduce costs/gain advantage for Chinese companies and negatively impact the U.S. economy?**

As I explained in my written testimony, Chinese companies can leap-frog ahead in technologies or products that they are unable to develop independently by stealing intellectual property; they can save money, time and human capital on

research and development; and they can move right from theft to the production of goods without spending time or money on product development. Also, companies that steal intellectual property in China may benefit from government subsidies and from government procurement programs, which save them money and ensures a market for products.

5. **China is pursuing a comprehensive long-term strategy to modernize its military and investing in ways to overcome the U.S. military advantage. Cyber espionage is regarded as the greatest tool in that effort, as the Pentagon noted this May in a report to Congress on China. In that report, for the first time, the Pentagon specifically named the Chinese government and military as the culprit behind intrusions into government and other computer systems. Is this a bell-weather moment for U.S.-China relations?**

No, I do not think naming the Chinese government and military as the perpetrator of cyber espionage is a bell-weather moment for U.S.-China relations. The Executive Branch and Congress complain all the time to Chinese officials about different practices in China. Most often, these complaints have no effect on Chinese policy. Taking action against China for this through legislation, executive order, or action by Congress to revoke permanent normal trade relations for China would be a bell-weather moment in U.S.-China relations.

6. **In your testimony, you recommend that the United States link Chinese economic espionage to "trade restrictions and bilateral issues." How would these restrictions fit within the regime of the World Trade Organization (WTO)? Could the WTO be used as a forum for addressing some of these issues?**

There are existing provisions in U.S. law, for example, Section 337 of the Trade Act of 1930 that provide some ability to address products that result from violations of intellectual property. The utility of existing provisions in U.S. law should be thoroughly examined and steps might be taken to update and reform these laws to enhance their utility. The WTO could be a forum for addressing some of these issues, but its utility is often limited by a time-consuming and cumbersome process. Updating its rules, with the failure of the ongoing Doha Round of negotiations appears to be limited and is also constrained by the consensus-nature of decision-making. But, every avenue should be examined to address this critical area.

7. **In your testimony, you recommend that the US government, military, and cleared defense contractors implement measures such as "meta-tagging, watermarking, and beaconing." What would these measures do to improve or protect against cyber theft or espionage? Why aren't these measures already in place?**

Meta-tags could be effective in identifying pirated or stolen intellectual property; however, actions like meta-tagging or watermarking alone are not enough. To be effective, there must be modern laws that would allow for criminal or civil action against violators. I don't believe our intellectual property protection and

economic espionage laws have kept up with the technology. Beaconing would help locate the violator and find where the stolen intellectual property resides. I don't know why such measures are not already in place. That question would have to be directed to software designers and the community of attorneys who work with them. If such measures were in place, however, there would have to be criminal or civil laws that would permit companies to go after thieves.

8. **In your testimony, you recommend that the United States government "prohibit Chinese firms using stolen US intellectual property from accessing US financial markets." Have you raised this recommendation with the Administration? What was the response? Given China's significant role in US financial markets (including the market for US Treasuries), do you see the potential for retaliation? Why or why not? Do the potential benefits of such a policy outweigh the potential effects of retaliatory measures?**

The Commission is a body established by Congress to report to Congress. I have not raised these matters with the administration. However, I note that up to this point, no U.S. Trade Representative has sent a panelist or witness to any of the Commission's hearings when they have been invited to do so. China invests in the U.S. for its own purposes.

In my view, it would be a good thing if equity investments by China were reduced. As for securities, the Commission's hearings on Wall Street have convinced me that China's investments in U.S. securities are a small part of the total U.S. bond market. If China moved that money all at once, there might be a slight effect on interest rates, but where would they put the money that is as secure? Most bankers that have testified before the Commission think this is an idle threat.

9. **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 President should use his executive powers to sanction companies and individuals in China that engage in this massive cyber espionage. Also our criminal and civil laws should be reviewed and updated to ensure that action can be taken against violators.

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?**

The government can help industry in all sectors with information on best practices and with security measures. Congress can pass legislation that has strong criminal penalties for engaging in these activities.

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?**

No, I think that in the case of intra-state critical infrastructure, the states must decide what parts of the energy industry are critical and they must set minimum standards that protect the citizens of the state from the catastrophic loss of that infrastructure to cyber-attack. In the case of inter-state critical infrastructure, when the loss of one section might have cascading, catastrophic effects on other states or the nation, the federal government must set minimum standards that industries must meet. For private companies that are not part of the defense industrial security program and are not part of the infrastructure critical to the nation, the government can provide help, and those industries can pick and choose in ways that they feel mitigate their risk in the most cost-effective way.

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?**

I think some industries have worked very hard on the problem and may be ahead of the federal government in some areas. How much they work together probably depends on proprietary matters, cost, and competitiveness, among other things.

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

Private industries and citizens have the main role in protecting their own property. It is up to government to provide them an adequate legal framework to do so, to provide adequate law enforcement, and to ensure that the measures people and companies take to protect their own property do not employ illegal or excessive force, brutality, or destructive measures. These are basic public policy matters.

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)?**

Legislation could require government agencies to establish specific programs to help with information sharing. But outside of national critical infrastructure and

defense-related programs, I think it is not possible to require information sharing. Nor would it be easy to verify compliance with information sharing requirements.

The Honorable Paul D. Tonko

1. **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?**

   Companies make their own decisions on how much risk their company can tolerate, how to mitigate that risk, and will decide on risk versus gain in China. Some may sacrifice intellectual property for market access or market share. Regardless of the outcome, corporations should be informed of the government's assessment of risk and they should have to live with the results of their decisions without relying on some government bailout.

2. **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?**

   From what I have seen so far, the fusion centers involving multiple agencies of government are doing a decent job of identifying threats. I do not believe that there is an adequate structure to investigate intellectual property theft, and it would be up to Congress to define and fund such a structure. As for new authorities, I suggested a few in my written and oral testimony. Action like meta-tagging and watermarking could be effective in identifying pirated or stolen intellectual property; however, actions like meta-tagging or watermarking alone are not enough. To be effective, there must be modern laws that would allow for criminal or civil action against violators. I don't believe our intellectual property protection and economic espionage laws have kept up with the technology. Beaconing would help locate the violator and find where the stolen intellectual property resides. I don't know why such measures are not already in place. That question would have to be directed to software designers and the community of attorneys who work with them. If such measures were in place, however, there would have to be criminal or civil laws that would permit companies to go after thieves.

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 based on the relevant excerpts from the hearing transcript regarding these requests are provided below.

The Honorable Michael C. Burgess

1. **You testified that you have had success with regards to the bilateral credit card and bank crime prevention. In order to protect the smaller banks, is there a way to involve the larger offshore banks that are doing these offshore transactions?**

From meetings with Federal Bureau of Investigation legal attaches and Department of Treasury representatives in Hong Kong and China, my understanding is that Chinese security authorities have been relatively helpful in pursuing criminal cases related to banking and credit card theft. These U.S. officials did not qualify their remarks by saying whether the cooperation is limited only to large banks or how responsive Chinese authorities are to criminal cases involving small banks. This question is best directed to the Departments of Justice and Treasury. The Internal Revenue Service also is involved in identifying and regulating offshore banking practices; IRS also may be able to respond to this question.

Thank you for the opportunity to respond to these questions. If I can be of any assistance in matters regarding cyber-security and the theft of American intellectual property please contact me.

Sincerely,

Larry M. Wortzel, Ph.D.
Commissioner

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

James A. Lewis
Center for Strategic and International Studies
Questions for the Record (QFR) from the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, Hearing of July 9, 2013

QFR – Congressman 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?

   Companies have developed a range of strategies to protect heir intellectual property during the manufacturing phase n China, including keeping the most sensitive processes outside of China, not providing the full package of IP used to make the product, ad lmit8ing Chinese employees access to IP.

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

   The most common tactic used by China to steal IP is "phishing," where a spoofed email is sent to company employees with an attachment (such as a video or spreadsheet) that infects the company network when it is opened. A second technique uses malicious websites, which contain malware that is automatically downloaded when the website is visited. Hackers attract visitor s by using common search terms, such as "Gangnam Style" or popular ring tones to get victims to visit the site.

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

      While the PLA assessment of US cybersecurity is not known, their actions indicate that they hold it in low regard, since they often use only the most basic hacking techniques and still succeed against many US companies.

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

      Tactics have change in recent years, growing more sophisticated. Attacks come in stages where the hackers first gain entry, then take control, and then exfiltrate information. The most advanced malware now may also use encryption to hide some its features and to make attribution more difficult.

3. What is our biggest leverage against the Chinese for their acts of cyber espionage?

   China does not wish to damage either economic or military relations with the U.S. This means that if they decide the U.S. is serious in its objections to cyber espionage, they will change their behavior.

   a. What role do companies have in protecting themselves?

Companies owe their investors due diligence in protecting their networks. Some companies have not put in place the most basic defensive techniques. This is one reason why China has been so successful.

c. Are other countries raising the issue of cyber espionage with China through diplomatic channels?

Several European countries have raise the cyber espionage issue with China, the most notable being Germany, where Chancellor Merkel has complained to Chinese leaders.

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

China will only change if it faces persistent pressure from the US and its allies to stop economic espionage. This includes continued engagement at senior levels and, possible, retaliatory measures against known Chinese actors.

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?

China's transient for Marxism has been difficult in that the rule of law was badly damaged under Mao. Corruption is widespread in China, there is little respect for property rights or intellectual property protecting, and this environment encourages hacking. Chinese hackers also feel that the West owes China for the "Century or Humiliation' and western imperialism. Many Chinese know that returning to rule of law is essential for their countries development. The development of agreed international norms on responsible state behavior in cyberspace would help change Chinese behavior, as would promoting better compliance by china with existing agreements on trade and intellectual property protection.

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?

The U.S. needs to create a new Agency responsible for all aspects of cyber security (as was recommended in the December 2008 CSIS "Report on the Cybersecurity for the 44th Presidency). This agency could be modeled on USTR or on the National Counterterrorism Center, and existing authorities given the DNI would allow for this Center to be stood up quickly. To quote that report;

> "Twenty years ago, all the federal experts who protected cyber space, gathered together, would have made a rather small club. Today, hundreds of cyber experts of varying ranks are found all over government—a proliferation in numbers that reflects the growth of the Internet itself and our reliance on it. But while

cyberspace operates with a shared set of organizing principles, the human network too often resembles a large fleet of well-meaning bumper cars.

The central problems in the current Federal organization for cybersecurity are lack of a strategic focus, overlapping missions, poor coordination and collaboration, and diffuse responsibility. A new administration could put much time and effort into an attempt to revitalize or resuscitate the existing organizational structure, which was the product of a marriage between a decade-long process of accretion and an end-of-term response to crisis. Our view is that this effort would waste time and energy.

The Commission considered many options for how best to organize for cybersecurity. We grew to understand the importance of bridging across the federal agencies in order to leverage their knowledge to provide the best security for our nation. Improving cybersecurity will be difficult, as the problem cuts across agency responsibilities. We also recognized the importance of involving the private sector – the federal government cannot do this alone.

Many of our interviews encouraged us to think of a holistic approach to cybersecurity, one that looked beyond security alone and asked how best to enable and assure essential services in cyberspace. The progression of out thinking led from an improved DHS to an expanded cybersecurity function in the NSC; from an expanded NSC to a new cybersecurity entity; and from a new cybersecurity entity to one that looked broadly at enabling the secure and reliable use of cyberspace for national functions."

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 U.S. needs to put more effort into creating a cybersecurity workforce. Currently there is a shortage of individuals with needed skills. Universities could play an important role in this, noting that traditional computer science programs are often not adequate for cybersecurity. Programs at junior colleges could also help meet workforce needs.

QFR – Congressman 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?

   Seeing a robust Cybersecurity Framework emerge from the February 2013 Executive Order is the most important thing that can be done to make Critical Infrastructure more secure. NIST should be encouraged to draw upon the experience of the Australian government, which has developed a number of mitigation strategies that greatly reduce risks. Another set

of generally principle of minute prescriptive guidance from NIST will not help. In addition, progress in removing impediments to information sharing are also important and the eventual passage of legislation like the House Bill CISPA would improve the situation.

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?

   Prescriptive regulations are unnecessary, but left to their own devices companies may not always choose the best approach. Current industry best practices are, judging from the very high number of successful attacks, inadequate It is important to set a standard for due diligence which critical infrastructure companies must meet. How companies meet these standard should be left them to them to choose.

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?

   Very little has been done to address cyber espionage by anyone. The financial sector has made substantial efforts, but their focus is on cyber crime, not espionage.

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

   Corporations owe a duty of care to their shareholders to protect their asset, including intellectual property. Increasingly, companies will incur liability risks if they do not put adequate cybersecurity measures in place. We can now definitely state the minimal requirements for cyber security (found in guidance like the Australian Signals Directorate's 35 Mitigation Strategies) and companies will need to take these into account if they are to exercise du diligence.

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)?

   Information sharing is problematic now because of legislative framework governing privacy is outdated, written for dial telephones and cooper wires. Information sharing cannot be improved or make its full potential contribution to cybersecurity without the passage of legislation like CISPA.

QFR – Congressman 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.?

China continues to struggle with creating an innovation economy, because of weak IP protections and political constraints. The 'innovation engine" in the U.S., however, is slowing done due to a combination of funding constraints, political obstacles, and regulatory burdens. This slowing of innovation in the U.S. puts America's technological leadership at risk. Until we change this situation, the U.S. will continue to slow in productivity growth, manufacturing, and innovation.

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?

   Companies appear to be reconsidering the risks of investing in China, in part because of the risk of intellectual property theft. The larger issue is how to get China to follow the "rules" created for international trade so that foreign companies can safely do business in that country.

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?

   Until recently, the U.S. has not done anything to stop Chinese cyber espionage. Recent initiatives by the administration have begun to change, this, but they will require persistence and perhaps sanctions to make progress. This will not be an easy struggle. As part of this effort, the U.S. should consider visa restrictions on Chinese individuals identified d as being involved in hacking, Treasury Department restrictions on the ability of such individual or Chinese companies involved in hacking to do business in the US or use the US financial system. The US could also consider indictments of suspected hackers and, as a final step, retaliatory trade measures. Other measures could include Other actions are also used to signal displeasure, such as canceling official visits, freezing visas issuance, or ending scientific cooperation. These steps al risk damaging the important trade relationship with China and they must be taken cautiously and in the context of a larger dialogue on cybersecurity, but if that dialog does not appear to be making adequate progress, sanctions must be used.

QFR – Congressman 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.

The Australian Signals Directorate (ASD), an intelligence agency responsible for cybersecurity, analyzed why the most frequent attacks succeeded. They found that most successful attacks exploited basic vulnerabilities. This led them to rank vulnerabilities by frequency and success rate and to develop strategies to mitigate these attacks. ASD used the information from its analysis to develop a list of 35 mitigation steps. The first four of these steps provide the greatest defensive benefit. One of the strengths of the ASD and NSA approach is that it is based on measurements and repeatable data. Another strength is that since most successful attacks consist of several steps that allow the hacker to penetrate the system and exfiltrate data, these measures interfere with one or more of these steps, effectively stopping known or unknown attacks when compared to the reactive approach used in other kinds of defense. A third strength is that the initial data suggest that these measures can actually save money when compared to existing practices. The data on these two strategies is compelling.

I was in Australia last week for a government law enforcement / intelligence conference and talked to the Australian Signals Directorate about their mitigation strategies. They provided me with talking points used by one of their senior officials who is responsible for Cyber and Information Security, on an experiment they ran on effectiveness:

---------- BEGIN ASD TALKING POINTS----------

I know many of you have heard the ASD mantra about what to do - implement the Top 4; Catch, Patch, Match. Here they are if they slipped your notice.

Someone posed the question, is "Catch, Patch, Match" just a marketing slogan?

So we ran an experiment to test whether the theory stood up in practice. What we were really interested in was seeing how the Top 4 went against real world malware.

We built 1200 virtual machines and we gathered together around 1700 malware samples. We used malware that had been employed against Commonwealth government agencies and also that lurking out in the wild of the internet.

Some of our machines had no Top 4 mitigations at all, some had the full dose, and the balance had varying degrees of mitigation.
We started by running malware on machines that had no mitigation. If they penetrated then they were run through the next, lightly mitigated machines. And so on to the machines with the Top 4 fully implemented.

The final result from our experiment, with the Top 4 mitigation strategies fully implemented, was … zero!

Now it is worth keeping in mind that the Top 4 will not … let me say that again … will not be effective against all malware. But they are an excellent step in improving cyber security.

----------END ASD TALKING POINTS----------

ASD summarized the experiment to me by noting that the combination of "White listing, least privilege user access, OS patching and application patching" was "Out of the 1700 samples - zero executed." In other words, all attacks were stopped. Australia has made the strategies mandatory for all government agencies. The US would benefit substantially if the ASD strategies were reflected in the Cybersecurity Framework being developed by NIST but there is some risk that this will not happen, given reluctance in the Administration to take advantage of the Australian experience. This would be unfortunate but is perhaps unavoidable at this time.

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

Ms. Susan Offutt
Chief Economist
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Offutt:

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 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

Attachment

August 7, 2013

Intellectual Property: *Additional Questions for the Record*

Dear Mr. Chairman:

It was a pleasure for GAO to appear before your subcommittee on July 9, 2013, to discuss our previous work on intellectual property counterfeiting, piracy, and cyber espionage. The enclosure is GAO's response to the subcommittee's questions for the record.

Sincerely yours,

Susan Offutt
Chief Economist, Applied Research and Methodology

Enclosure: Additional Questions for the Record

The Honorable Tim Murphy

Question 1: In your testimony you mention counterfeiting risks may lead to reductions in investment in R&D. Can you cite some recent examples?

Experts we spoke with in our 2010 report stated that companies could experience a decline in innovation and production of new goods if counterfeiting leads to reductions in corporate investments in research and development.[1] Similarly, the Organisation for Economic Cooperation and Development's (OECD) 2008 report cited loss of sales volume and lower prices as short-term effects, while the medium- and long-term effects include loss of brand value and reputation, lost investment, increased costs of countermeasures, potentially reduced scope of operations, and reduced innovation.[2] In our July 2012 testimony before this subcommittee, we provided a range of examples involving data loss or theft, economic loss, and privacy breaches.[3] In particular, 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. Subsequent to the reported breach, the company's stock fell more than 9 percent before trading in its stock was halted.

---

[1] GAO, *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*, GAO-10-423 (Washington, D.C.: April 12, 2010).

[2] Organisation for Economic Cooperation and Development (OECD), *the Economic Impact of Counterfeiting and Piracy*. Paris: OECD, 2008).

[3] GAO, *Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage*, GAO-12-876T (Washington, D.C.: June 28, 2012).

Question 2: It seems that neither government nor industry is able to solidly assess what the size and scope of the problem is. In your testimony, you state that "one of the key problems is that data have not been systematically collected and evaluated". How can this be improved? Is it possible to move forward with somewhat accurate data of incidents that allows for a basic understanding of the situation?

There are three possible sources of information and analysis that might help advance the understanding of the size and scope of the problem of intellectual property (IP) theft. One source is government, where those agencies that have responsibilities regarding enforcement of IP laws can provide statistics that might help inform the debate. For example, five key agencies play a role in IP enforcement: (1) Customs and Border Protection (CBP) and (2) Immigration and Customs Enforcement (ICE) of the Department of Homeland Security, (3) Federal Bureau of Investigation (FBI), (4) Food and Drug Administration (FDA), and (5) Department of Justice. Since we issued our 2008 report,[4] many agencies have implemented GAO recommendations to better assess data related to IP enforcement. For example, agencies have taken steps to better identify enforcement actions against IP-infringing goods that pose a risk to the public health and safety of the American people, and to collect and systematically analyze enforcement statistics to better understand variations in IP-related enforcement activity. In addition to our 2010 report on efforts to quantify the economic effects of counterfeit and pirated goods,[5] the International Trade Commission (ITC) conducted two studies regarding the effect on the U.S. economy and U.S. jobs of IP rights infringement in China. These studies were conducted in response to an April 2010 request from the United States Senate Committee on Finance.[6]

Another government source for understanding the scope of IP theft is the Intellectual Property Enforcement Coordinator (IPEC), a position created by the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act).[7] The act mandates IPEC to chair an interagency advisory committee and coordinate the committee's development of the Joint Strategic plan against counterfeiting and infringement. The joint strategic plan was required to address key elements of an effective national strategic plan. The PRO-IP Act required the IPEC to submit the joint strategic plans to specific committees of Congress every third year after the development of the first strategic plan. The Act also requires the IPEC to submit a report on the activities of the advisory committee during the preceding fiscal year. These reports provide information on the size and scope of the problem. Specifically, the joint

---

[4]GAO, *Intellectual Property: Federal Enforcement Has Generally Increased, but Assessing Performance Could Strengthen Law Enforcement Efforts*, GAO-08-157 (Washington, D.C.: Mar. 11, 2008).

[5]GAO-10-423.

[6]ITC, *China: Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the U.S. Economy*, Investigation No. 332-514, USITC Publication4199 (amended) (Nov. 20104. ITC, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*, Investigation No. 332-519, USITC Publication 4226 (May 2011).

[7]Pub. L. No. 110-403, 122 Stat. 4256

strategic plan is required to provide an analysis of the threat posed by violations of IP rights, including costs to the U.S. economy and threats to public health and safety. The annual report is required to report on, among other things, the progress made on implementing the strategic plan and progress toward fulfillment of the priorities identified in the joint strategic plan. In our 2010 report, we reported on the status of IPEC's efforts to implement the act.[8]

A second source of information that might help advance the understanding of the size and scope of the problem of IP theft are studies conducted by firms or their industry associations. In our 2010 report, we observed that assumptions such as the rate at which consumers would substitute counterfeit for legitimate products can have an enormous impact on the resulting estimates.[9] Nonetheless, these studies can provide insights on the nature of IP theft in particular markets or geographic locations and can help firms and others understand some of the patterns and characteristics of IP theft. The third source for information that might help advance the understanding of the size and the scope of the problem of IP theft are studies conducted by academic, public policy research organizations, and international groups. These entities have made significant contributions to understanding the impact of IP theft and its broader implications. For example, OECD released a report in 2008 examining the impact of counterfeiting and piracy on the global economy.[10]

Question 3: In your testimony, you highlight the importance of accurate data regarding the extent and value of counterfeit trade. You also highlight industry's frequent unwillingness to disclose such data. What privacy standards are necessary to improve disclosure by these entities?

GAO's work on IP enforcement has not examined whether government privacy standards would improve the disclosure of accurate data concerning IP theft. However, our 2010 report provided a few insights as to why industries are unwilling to disclose data regarding the extent and value of counterfeit trade.[11] We reported that industries that collect this information may be reluctant to discuss instances of counterfeiting because this might lead to consumers losing confidence in their products. Also,sharing information on IP theft could also provide opportunities for proprietary information to fall into the hands of competitors or those who are intent on infringing the firms' IP rights. In addition, OECD officials told us that one reason some industry representatives were

---

[8]GAO, *Intellectual Property: Agencies Progress in Implementing Recent Legislation, but Enhancements Could Improve Future Plans*, GAO-11-39 (Washington, D.C.: Mar. 11, 2008).

[9]GAO-10-423.

[10]Organisation for Economic Cooperation and Development (OECD), *The Economic Impact of Counterfeiting and Piracy* (Paris: OECD, 2008).

[11] GAO, *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*, GAO-10-423 (Washington, D.C.: April 12, 2010).

hesitant to participate in their 2008 study was that they did not want information to be widely released about the scale of the counterfeiting problem in their sectors because the presence of counterfeit products may damage the value of the brand and image of the producers of genuine products over time.

Question 4: How can the United States encourage China to adopt stricter policies on the protection of intellectual property (i.e., patent rights, copyright, infringement, trademark violations)?

In 2009, GAO issued a report examining efforts to enhance protection and enforcement of IP overseas and focused our work on four posts in three countries, including two posts in China: Beijing and Guangzhou.[12] We found that U.S. government officials had identified weak enforcement as a key IP issue in the three case study countries; however, weaknesses also persist in the countries' IP laws and regulations. According to the U.S. government, enforcement of existing IP laws and regulations and adjudication of suspected infringements are limited and inconsistent, and penalties are not typically sufficient to serve as an effective deterrent. U.S. government documents and U.S. officials we interviewed cited several factors that contribute to this limited and inconsistent enforcement, including flawed enforcement procedures; a lack of technical skills and knowledge of IP among police, prosecutors, and judges; a lack of resources dedicated to IP enforcement efforts; and the absence of broad-based domestic support for strong IP enforcement.

In our 2009 report, we also reported on the U.S. Patent and Trademark Office (USPTO) IP attaché program which was created to address country-specific and regional IP problems in key parts of the world.[13] USPTO's first IP attaché was posted in Beijing in 2004 and Guangzhou in 2007, along with the addition of IP attachés in several other countries. The IP attachés work on a range of IP activities in coordination with other federal agencies, U.S. industry, and foreign counterparts. According to USPTO, the IP attachés are tasked with advocating U.S. government IP policy, interests and initiatives; assisting U.S. businesses on IP protection and enforcement; improving IP protection and enforcement by conducting training activities with host governments; advising officials from other U.S. agencies on the host government's IP system; advising representatives of the host government or region on U.S. intellectual property law and policy; helping to secure strong IP provisions in international agreements and host country laws and working to monitor the implementation of these provisions; and performing limited commercial service duties as necessary, such as representing the commercial service at host government functions and advising U.S. companies on the local IP environment.

We found that the USPTO IP attachés at the four posts we visited were generally effective in collaborating with other agencies, primarily by acting as IP focal points, establishing IP working groups, and leveraging resources through joint activities. However, we reported that three of the four posts, including the two posts in China, had not adopted interagency plans to address key IP issues. Policy guidance on IP at the

---

[12] GAO, *Intellectual Property: Enhanced Planning by U.S. Personnel Overseas Could Strengthen Efforts*, GAO-09-863 (Washington, D.C.: Sept. 30, 2009).

[13] GAO-09-863

posts, such as the annual Special 301 report and embassy mission strategic plans, is high level and not generally used for planning agencies' day-to-day IP efforts. We reported that the three posts could potentially enhance collaboration by developing joint strategies to translate the key IP issues identified by the U.S. government into specific objectives and activities. For example, joint strategies could help agencies prioritize existing efforts, avoid duplication of efforts, formulate a common IP message to foreign governments, and maintain focus on IP given competing issues and personnel changes at posts. In response to our recommendation to develop annual work plans, the Department of State issued a cable in November 2009 to those posts with USPTO IP attachés at the time, noting the State's concurrence with our recommendation and directing post leadership to work with IP attaches to determine how to effectively apply our suggestions and implement the recommendation.

○