RPTS JANSEN

DCMN ROSEN

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, D.C.

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.

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. In a recent report by a cyber security consulting firm documented that

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 Kinetic, 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 Kinetic'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. experts 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 Secretary -- former Senator, sorry, 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 Mr. DeGette. You are recognized for 5 minutes.

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 having 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.

The Chairman. 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.

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, 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, 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.

Dr. 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.

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

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, okay. 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 wear 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. -- 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:]

******** INSERT 1-1 ********

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 property 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:]

******** INSERT 1-2 ********

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:]

******** INSERT 1-3 ********

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 -- 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:]

******** INSERT 1-4 ********

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, you know, 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, you know, 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. Thank the gentlelady. Now recognize Dr. Burgess for 5 minutes.

Dr. Burgess. Thank you, Mr. Chairman. And, yeah, 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 -- yeah, 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?

RPTS MCCONNELL

DCMN ROSEN

[11:13 a.m.]

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 --

Dr. 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.

Dr. 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.

Dr. 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.

Dr. 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. Yeah, 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.

Dr. Burgess. Can I just ask you a question on that? Because that --

Mr. Wortzel. Pardon me?

Dr. 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.

Dr. Burgess. Okay. 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.

Dr. Burgess. Yeah, 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. Yeah.

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 easier 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. Okay.

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 -- 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 -- somewhat easier, you know, to go to court and to get seizures. It's nowhere -- 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. Yeah. Well, my time is expired. I had much more I wanted to talk about, but maybe we will get that to 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 like -- not credible. It's based on first, the notion that the -- one-third of the economy is based on -- 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. Okay, 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, are you -- you know, 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, does -- do any other countries stand out as one that is perhaps doing it right, getting -- 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. Okay.

Mr. Gorton. We were interested in what we -- 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 in the -- 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 could coordinator in the White House. He 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. I will talk to Mr. Lewis. I have been in Pittsburgh, and I have seen a great side of injustice and theft. Might as well talk 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 own 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 -- of operators 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 yet, despite official denials we have been able to trace these attacks back to China. And so 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 infrastructure 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 we have invested billions of dollars in the Eagle Ford shale plate with American partners, and I suspect they are trying to get that technology from the drill bit technology, other things, hydraulic fracturing because they have shale plates in Western China. It's a very different 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 of the firm level. I mean, that's the way we would aggregate to a number that told us something meaningful about the extent of both

what is at risk, what has been compromised, and then how it has been used to affect firm sales or consumer purchases. And that is quite data- and labor-intensive, but presumably, it may -- some of those data may come 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 -- the staff, 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 -- 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 a -- 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 objection, so hearing no objection, so ordered.

[The letter follows:]

******** COMMITTEE INSERT ********

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.]