AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 113–780

ECONOMIC ESPIONAGE AND TRADE SECRET THEFT: ARE OUR LAWS ADEQUATE FOR TODAY'S THREATS?

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

MAY 13, 2014

Serial No. J–113–59

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PUBLISHING OFFICE

96–009 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing 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 THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

DIANNE FEINSTEIN, California
CHUCK SCHUMER, New York
DICK DURBIN, Illinois
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
AL FRANKEN, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut
MAZIE HIRONO, Hawaii

CHUCK GRASSLEY, Iowa, *Ranking Member*
ORRIN G. HATCH, Utah
JEFF SESSIONS, Alabama
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TED CRUZ, Texas
JEFF FLAKE, Arizona

KRISTINE LUCIUS, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON CRIME AND TERRORISM

SHELDON WHITEHOUSE, Rhode Island, *Chairman*

DIANNE FEINSTEIN, California
CHUCK SCHUMER, New York
DICK DURBIN, Illinois
AMY KLOBUCHAR, Minnesota

LINDSEY GRAHAM, South Carolina, *Ranking Member*
TED CRUZ, Texas
JEFF SESSIONS, Alabama
MICHAEL S. LEE, Utah

AYO GRIFFIN, *Democratic Chief Counsel*
DAVID GLACCUM, *Republican Chief Counsel*

CONTENTS

MAY 13, 2014, 2:34 P.M.

STATEMENTS OF COMMITTEE MEMBERS

	Page
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont, prepared statement	28
Whitehouse, Hon. Sheldon, a U.S. Senator from the State of Rhode Island	1
prepared statement	29

WITNESSES

Witness List	27
Coleman, Randall C., Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, Washington, D.C.	4
prepared statement	31
Greenblatt, Drew, President and Owner, Marlin Steel Wire Products, Baltimore, Maryland	12
prepared statement	87
Hoffman, Peter L., Vice President, Intellectual Property Management, The Boeing Company, Chicago, Illinois	8
prepared statement	38
Norman, Douglas K., Vice President and General Patent Counsel, Eli Lilly and Company, Indianapolis, Indiana	14
prepared statement	94
Passman, Pamela, President and Chief Executive Officer, Center for Responsible Enterprise & Trade (CREATe.org), Washington, D.C.	10
prepared statement	47

QUESTIONS

Questions submitted to Randall C. Coleman by Senator Whitehouse	99
Questions submitted to Peter L. Hoffman by Senator Flake	100
Questions submitted to Douglas K. Norman by Senator Flake	101
Questions submitted to Pamela Passman by Senator Flake	102

ANSWERS

Responses of Randall C. Coleman to questions submitted by Senator Whitehouse	103
Responses of Peter L. Hoffman to questions submitted by Senator Flake	105
Responses of Douglas K. Norman to questions submitted by Senator Flake	106
Responses of Pamela Passman to questions submitted by Senator Flake	107

ECONOMIC ESPIONAGE AND TRADE SECRET THEFT: ARE OUR LAWS ADEQUATE FOR TODAY'S THREATS?

TUESDAY, MAY 13, 2014

UNITED STATES SENATE,
SUBCOMMITTEE ON CRIME AND TERRORISM,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:34 p.m., in Room SD–226, Dirksen Senate Office Building, Hon. Sheldon Whitehouse, Chairman of the Subcommittee, presiding.

Present: Senators Whitehouse, Coons, Graham, Hatch, and Flake.

OPENING STATEMENT OF HON. SHELDON WHITEHOUSE, A U.S. SENATOR FROM THE STATE OF RHODE ISLAND

Chairman WHITEHOUSE. The hearing of the Senate Judiciary Subcommittee on Crime and Terrorism will come to order. I am expecting that my Ranking Member, Senator Lindsey Graham, will be here shortly, but I just saw him on the C-SPAN screen, so I know that he is on the floor and not here. But I have permission from his staff to proceed, and he will join us as soon as his schedule permits.

I also want to recognize in the audience Ed Pagano, who has spent many a happy hour in here when he was working for Chairman Leahy. It is good to have him back in a different capacity.

We are having a hearing today that is entitled "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?" Today the Subcommittee is going to explore how we can better protect American businesses from those who try to steal their valuable intellectual property.

American companies are renowned as being the most innovative in the world. Companies of every size and in every industry, from manufacturing to software to biotechnology to aerospace, own large portfolios of legally protected trade secrets they have developed and innovated. In some cases, the "secret sauce" may be a company's most valuable asset. The theft of these secrets can lead to devastating consequences. For small businesses it can be a matter of life and death.

The risk of trade secret theft has been around as long as there have been secrets to protect. There is a reason why Coca-Cola has kept its formula locked away in a vault for decades. But in recent years, the methods used to steal trade secrets have become more

sophisticated. Companies now must confront the reality that they are being attacked on a daily basis by cyber criminals who are determined to steal their intellectual property.

As Attorney General Holder has observed, there are two kinds of companies in America: Those that have been hacked and those that do not know that they have been hacked.

Today a criminal can steal all of the trade secrets a company owns from thousands of miles away without the company ever noticing. Many of the cyber attacks we are seeing are the work of foreign governments. China and other nations now routinely steal from American businesses and give the secrets to their own companies—their version of competition.

And let us be clear. We do not do the same to them. We are now going through a healthy debate in America about the scope of government surveillance, but there is no dispute about one thing: Our spy agencies do not steal from foreign businesses to help American industry.

While cyber attacks are increasing, traditional threats remain. Company insiders can still walk off with trade secrets to sell to the highest bidder. Competitors still steal secrets through trickery or by simply breaking into a factory or office building.

It is impossible to determine the full extent of the loss to American businesses as a result of the theft of trade secrets and other intellectual property. There have been estimates that our Nation may lose anywhere from one to three percent of our gross domestic product through trade secret theft alone.

The Defense Department has said that every year an amount of intellectual property larger than that contained in the Library of Congress is stolen from computer networks belonging to American businesses and government. And estimates of the value of IP stolen by foreign actors are as high as $300 billion.

General Keith Alexander, until recently the head of NSA and of Cyber Command at the Pentagon, has characterized the cyber theft of American intellectual property as, I will quote, "the greatest transfer of wealth in history." And, of course, we are on the losing end of it.

But no estimate can fully capture the real impact of trade secret theft because when other countries and foreign businesses steal our trade secrets, they are stealing our ideas. They are stealing our innovation. Most importantly, they are stealing our jobs.

In my own State of Rhode Island, we continue to face unacceptably high unemployment, despite having some of the most innovative businesses in the country. If we do not protect our businesses from those who steal their intellectual property, then we are letting that innovation go to waste, and we are letting American jobs go overseas.

In the past, some companies were reluctant to talk about this issue because no one likes to admit that they have been victimized. But many are now coming forward to speak out because they recognize how important it is that we work together to address this common threat.

I particularly want to thank the company representatives who are appearing before us today in the second panel as well as many,

many others who have worked closely with me and with other Senators on this issue.

I am encouraged that the administration last year released a blueprint for a strategy to combat trade secret theft, and agencies across the government are increasing efforts to address this problem. The administration must recognize that the theft of intellectual property is one of the most important foreign policy challenges we face, and it must communicate to China and other nations that stealing from our businesses to help their businesses is unacceptable.

We in Congress must do our part. We need to make sure that our criminal laws in this area are adequate and up to date. Last fall, Senator Graham and I released a discussion draft of legislation designed to clarify that state-sponsored overseas hacking could be prosecuted as economic espionage and to strengthen criminal protection of trade secrets.

We received valuable comments and suggestions about this legislation, and we look forward to hearing from our witnesses today about how to improve our laws and what we can do to help defend our industries. And we hope to introduce our legislation in the coming weeks.

Companies also need civil remedies against those who steal from them. While State law has traditionally provided companies with remedies for misappropriation of trade secrets, there is currently no Federal law that allows companies themselves to seek civil remedies against those who steal from them. Senators Coons and Hatch have recently introduced legislation to give victims of trade secret theft the option of pursuing thieves in Federal court. Senator Flake has also introduced legislation to give companies a Federal civil remedy for trade secret theft. I hope that the Judiciary Committee will act soon on legislation to strengthen both the criminal and civil protections against trade secret theft, and I look forward to working with those colleagues toward that goal.

Today we will hear from witnesses in government, industry, and the nonprofit sector who confront the threat of trade secret theft on a daily basis. What I hope will be clear by the end of this hearing is that we need an all-in approach to this hearing. We must strengthen our criminal laws, and our law enforcement agencies must prioritize stopping trade secret theft before it occurs, and investigate it and prosecute it when it does occur.

I will add that there remains an urgent need for us to pass broader cybersecurity legislation, and I appreciate working with Senator Graham on that effort.

I look forward to hearing from our witnesses today and to working with my colleagues on both sides of the aisle to address this critical issue.

Our first witness is Randall C. Coleman, the Assistant Director of the Counterintelligence Division at the Federal Bureau of Investigation. Mr. Coleman is responsible for ensuring that the FBI carries out its mission to defeat foreign intelligence threats. Mr. Coleman began his career as a special agent with the FBI in 1997 and has previously served as assistant special agent in charge of the San Antonio Division, chief of the Counterespionage Section, and special agent in charge of the Little Rock Division. Prior to his ap-

pointment to the FBI, Mr. Coleman served as an officer in the United States Army for nine years. We are delighted that he could join us today, and we ask him to proceed with his testimony.

[The prepared statement of Senator Whitehouse appears as a submission for the record.]

Proceed, sir.

STATEMENT OF RANDALL C. COLEMAN, ASSISTANT DIRECTOR, COUNTERINTELLIGENCE DIVISION, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, DC

Mr. COLEMAN. Good afternoon, Chairman Whitehouse. I am pleased to be here today with you to discuss the FBI's efforts to combat economic espionage and theft of trade secrets.

The FBI considers the investigation of theft of trade secrets and economic espionage a top priority. In 2012 alone, the National Counterintelligence Executive estimated a range of loss to the U.S. economy approaching $400 billion to foreign adversaries and competitors who, by illegally obtaining a broad range of trade secrets, degraded our Nation's advantage and innovative research and development in the global market. This immense loss threatens the security of our economy, and preventing such loss requires constant vigilance and aggressive mitigation.

The FBI is diligently working to investigate and apprehend targets pursuing economic espionage against U.S.-based businesses, academic institutions, cleared defense contractors, and government agencies, and has made significant progress in putting some of the most egregious offenders behind bars.

Economic espionage and theft of trade secrets are increasingly linked to the insider threat and the growing trend of cyber-enabled trade secret theft. The insider threat employee may be stealing information for personal gain or may be serving as a spy to benefit other organizations or country. Foreign competitors aggressively target and recruit insiders to aid the transmittal of a company's most valued proprietary information.

The FBI, however, cannot protect the Nation's economy by acting alone. The FBI Counterintelligence Division's Strategic Partnership Program oversees a network of more than 80 special agents that are serving as strategic program coordinators who work hand in hand with industry and academic institutions across the country. These strategic partnership coordinators conduct in-person classified and unclassified threat presentations and briefings, and it serves as an early referral mechanism for reports of possible economic espionage, theft of trade secrets, and cyber intrusions.

Working through the more than 15,000 contacts nationwide, this program helps companies detect, deter, and defend against attacks of sensitive proprietary information from our foreign adversaries.

The FBI takes seriously its role to investigate and apprehend targets pursuing economic espionage, and by forming close partnerships with local, logical businesses and academic and government institutions, the FBI wishes to have a greater impact on preventing and deterring the loss of trade secrets before any loss can actually occur.

Thank you again for the opportunity to testify, and I look forward to answering any of your questions, sir.

[The prepared statement of Mr. Coleman appears as a submission for the record.]

Chairman WHITEHOUSE. I would like to talk with you about a couple of things.

First of all, have you any specific reaction to the draft legislation that Senator Graham and I circulated for discussion purposes?

Mr. COLEMAN. Sir, I will stand on this: That any legislation that allows the FBI to have a better advantage at going after our foreign adversaries as it relates to economic espionage and theft of proprietary information, the FBI is in favor of.

Chairman WHITEHOUSE. And presumably the people we are working with at the Department of Justice, do you support the——

Mr. COLEMAN. Yes, sir.

Chairman WHITEHOUSE [continuing]. Arguments and points that they are making?

Mr. COLEMAN. Absolutely.

Chairman WHITEHOUSE. One of the things that I have observed, having watched this for a while, is that whenever I hear about a case that is brought for intellectual property theft, in every case that I have found so far there has been some nexus to old-fashioned type intellectual property theft—somebody taking the DVD home, somebody taking the patented item out of the factory.

We have seen an explosion in pure cyber intrusions and extraction through the cyber network of intellectual property with no other technique involved. And to my knowledge, there have been no charges brought ever against anyone for that kind of activity.

I understand that these cases are very complicated. I understand that they have huge forensic issues, that there is an overlay with national security and with the intelligence services that requires a lot of effort. I understand that some of the targets are overseas, and that creates a whole other array of legal and other issues.

Trust me, having served as a United States Attorney, I can see how very challenging these cases are to make. But when you have General Alexander saying that we are on the losing end of the biggest transfer of wealth in human history, you would like to see a little bit more actual hard prosecution activity.

Can you tell me what you think is behind that difficulty? And is there anything that we can do? Is it just a resource question? What can we do in Congress to start putting some points on the board against these people in criminal law courts?

Mr. COLEMAN. Chairman, I think you described it to a T. Obviously when you get outside of the borders of the United States, in many of these investigations where there is a foreign nexus, our ability to conduct effective investigations is diminished greatly.

I will tell you that we do have ongoing investigations that I would foresee as having a logical conclusion that I think you would agree that are as you described. In fact, the FBI has actually placed cyber assets and resources working with the counterintelligence resources at our National Cyber Intrusion Task Force that are working hand in hand and shoulder to shoulder on these specific investigations.

So I think technology plays a critical role, and the advancement of technology makes the threat that much more complicated. But I think there has been tremendous progress made by the FBI along

with our partners at investigating these type of crimes, and so I am hopeful as we go forward that we will be able to demonstrate that we have been effective and will be effective in this arena.

Chairman WHITEHOUSE. I would not want to suggest that the FBI has not been effective. I have been out to the NCIJTF. I have seen what you guys do out there. If I had to take my concern and turn it into just a single phrase, it would not be the FBI is not effective. It would be: The FBI is so busy trying to keep track of who is coming through the doors and coming through the windows and trying to warn all the companies that they are hacking into that there simply is a resource constraint in terms of taking all that effort, which could be devoted to tracking all these attacks and trying to help our businesses, there just is not the capability or enough capability to sit down and go through putting a prosecution package together, working it through the intelligence agencies, and doing all the other steps that need to be done.

So in many ways, I am trying to throw you a friendly question saying let us help you do what needs to be done in terms of the resources. I would not want to take anybody off of what they are doing out at NCIJTF in order to put a prosecution package together. But at some point, we have to have a robust enough response to this problem as a country that we are starting to, for want of a better example, indict Chinese colonels and generals who are behind pulling this kind of thievery off.

Mr. COLEMAN. I think another part of what I think is important—and you described it—is the threat is so immense that that is what makes this outreach effort so important to what we are doing and bringing in the private sector and the academic institutions to work hand in hand with us so we can actually try to get out in front of this threat.

But you are absolutely right. The threat is so immense that the FBI cannot take this on alone, and whatever necessary help that we can get in those other industries and sectors is of great help to us.

Chairman WHITEHOUSE. There is a provision in the last appropriations bill that requires the Department of Justice to do a report for us, looking forward, looking out a couple years, and thinking about what the structure should be like for addressing this particular threat. It has exploded, as you know. And it explodes even further every year. It grows just at massive levels.

I am not convinced at this point that the present set-up makes sense. And if you look at another area that exploded, if you look at what happened when aviation began and what its effect was on the conduct of warfare, you started with the Army air effort as a subpart of the Signal Corps. And then it became a subpart of the Army, and it was not really until after World War II that you had a full-on U.S. Air Force. And since then we have been a very successful leader in that theater of military operations. But until then we really were not set up right.

I am not convinced that we are set up right, and I would invite you to comment on this. But let me also ask it as a question for the record that you can take back to headquarters. How does it make sense to have these kind of cases, perhaps in your Counterintelligence Division, perhaps in the Cyber Division, perhaps in the

Criminal Division, how do you sort amongst those three Divisions to have this be efficient and smooth flowing? Because I understand that each of those different sections has a piece of this.

Mr. COLEMAN. I think the first part of your comment is: Are we structured right? And I will tell you that I look at this on a daily basis. It is certainly a priority for our Director to look at are we efficiently and effectively addressing the threats. And I will tell you in the Counterintelligence Division, economic espionage has become a priority because of the expansion of the threat.

So there are always ways that we are looking to better address this, and some of the more significant efforts that we have made is to really have outreach, and I cannot stress how important that is to this process and what benefits we have seen from that.

We have expanded our contacts across the country to 15,000 contacts. We are conducting over 7,800 presentations and briefings a year. And we are starting to see—the maturity of these relationships is starting to pay off in the fact that companies are starting to come to us, academic institutions are actually coming to us early on and calling that contact so we can get engaged in the problem at the very early period, versus after a bad actor has left the company with two or three terabytes of information has already left.

So that is absolutely a victory for us in this process, but we have a lot of room for improvement that we will continue to do. And we are always looking at ways to improve that.

Chairman WHITEHOUSE. Well, in the context of that, if you could take it as a question for the record and get an official response from your organization, I am interested in whether you think, you know, five years out, 10 years out, that similar division across all those separate parts of the Bureau will continue to be a wise allocation or whether we are in sort of a transient step toward what ultimately will be the way we address this.

Mr. COLEMAN. Yes, Mr. Chairman, I understand.

Chairman WHITEHOUSE. Terrific.

[The information referred to appears in Answers as a submission for the record.]

Chairman WHITEHOUSE. Thank you for your service. I know that this is an immensely challenging area that calls on all sorts of different resources, and I am proud of the way the FBI conducts itself in this area, and I appreciate your service to our country.

Mr. COLEMAN. Mr. Chairman, thank you very much for having me today.

Chairman WHITEHOUSE. We will take a two-minute recess while the next panel gets itself sorted out and come back into action then.

[Pause.]

Chairman WHITEHOUSE. All right. The hearing will come back to order, and I thank the witnesses for attending and participating in this hearing. We have a terrific panel of witnesses, and I am delighted that you are all here. This is very promising.

Peter Hoffman is the Vice President of Intellectual Property Management for The Boeing Company, which has plenty of intellectual property to manage. He has worked there since 1984. In his current role, he manages the company's patent portfolio, protection of its trade secrets, and licensing of technical data images, con-

sumer products trademarks, and patents. Prior to being appointed to his current position, Mr. Hoffman served as the Director of Global Research and Development Strategy for Boeing Research and Technology, which is the company's advanced research organization. We welcome him, and why don't you give your statement, and I will introduce and take the statement of each witness, and we will open it for questions after that.

Please proceed, Mr. Hoffman.

STATEMENT OF PETER L. HOFFMAN, VICE PRESIDENT, INTELLECTUAL PROPERTY MANAGEMENT, THE BOEING COMPANY, CHICAGO, ILLINOIS

Mr. HOFFMAN. Good afternoon, Chairman Whitehouse. On behalf of The Boeing Company, I thank you for convening this hearing, and I am grateful for your leadership on efforts to improve trade secrets laws. It is a privilege to be a participant on this panel and provide Boeing's view on the challenges faced by America's innovators.

Boeing first began making twin-float airplanes in 1915 from a small red boathouse in Seattle, and while much has changed since then, our company remains unique in that we assemble, test, and deliver most of our highly competitive products right here in the United States. The final assembly facilities for our commercial products are located in the States of Washington and South Carolina, but we have facilities for engineering and manufacturing of major components in multiple States, including Oregon, Florida, California, Montana, and Utah. Our defense and space-related production is primarily located in the States of California, Missouri, Pennsylvania, Texas, Arizona, Florida, and Alabama.

Today, Boeing employs 160,000 people across the United States. Since 2005, we have created more than 15,000 new, high-paying jobs driven by our record backlog of over 5,000 commercial airplanes. Last year we paid $48 billion to more than 15,600 U.S. businesses, which collectively support an additional 1.5 million jobs across the country.

Boeing's significant contribution to the U.S. economy today, and for the past 100 years, is the result of the ingenuity of our highly skilled employees. Innovating each step of the way, they develop the most sought-after products and technologies in the world. Boeing's cutting-edge technologies take years to develop at an enormous expense, approximately $3 billion of research and development spent per year, and the bulk of our innovations are protected as trade secrets.

Because of this, trade secret protections are vital to securing Boeing's intellectual property. Boeing does not simply have one recipe for its secret sauce; we have thousands of trade secrets that are critical to maintaining our unparalleled success. Unfortunately, Boeing's valuable engineering and business information is at significant risk. Once publicly disclosed, rights in trade secrets may be lost forever, the investments wiped out in an instant along with the competitive advantage those trade secrets provided.

Of course, Boeing is on constant guard to prevent the theft of our trade secrets, but today companies cannot simply lock their trade secrets in a safe. The vast majority of our business and engineering

information is stored electronically. The digital age has brought great gains in productivity but also has increased risk. At any moment we could lose a trade secret, through a breach in our network, through disclosure by one of our employees or partners, or through an escape at one of our many suppliers' facilities.

Fear of trade secret theft is not a concern just for Boeing. Middle- and small-size companies that rely on trade secrets have as much or more to fear as big companies, particularly if their survival depends on a single product or service.

Given the risk U.S. companies face every day, more needs to be done to deter thieves from stealing our trade secrets. This theft is a crime, and we must send a clear message that we will not stand by as thieves harm our businesses, hurt our economy, and steal our jobs. Thus, we strongly support your efforts, Chairman Whitehouse, and also the efforts of Ranking Member Graham to call attention to the issue and to provide law enforcement with additional tools to deter trade secret theft.

The Uniform Trade Secrets Act provides a general framework for State legislatures to adopt trade secret protections, but the standards and procedures adopted can vary from State to State, and jurisdictional issues may complicate matters further. As such, it is a real concern of U.S. companies that State action under the Uniform Trade Secrets Act may not, in some cases, be immediate enough to prevent the loss of a trade secret.

So we also acknowledge the need for companies to have the ability to take immediate action of our own in Federal court to prevent the loss of our valuable trade secrets when State courts and Federal law enforcement cannot act quickly enough.

Therefore, we would also like to thank Senator Coons and Senator Hatch for introducing the *Defend Trade Secrets Act* and your efforts to establish the right for a company to file an application in a Federal district court in order to seize property containing trade secrets stolen from a company. We look forward to working with Senator Coons and Senator Hatch on this bill and supporting your efforts to encourage the Congress to act quickly to pass this important legislation.

We are also encouraged that the new laws under discussion, if passed, will strengthen overseas trade secret enforcement by raising awareness of the issue, promoting cooperation between U.S. and foreign law enforcement, and empowering our trade negotiators to encourage our trading partners to similarly raise the bar.

In conclusion, we applaud your efforts to highlight this issue and to strengthen U.S. trade secret laws, and thereby help protect our valuable assets.

Thank you for your time in hearing our concerns.

[The prepared statement of Mr. Hoffman appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you, Mr. Hoffman. I appreciate your testimony.

Our next witness is Pamela Passman, the president and CEO of the Center for Responsible Enterprise & Trade, also known as CREATe.org. CREATe is a global nongovernmental organization dedicated to helping companies and supply-chain members imple-

ment leading practices for preventing corruption and protecting intellectual property.

Prior to founding CREATe in October 2011, Ms. Passman was the corporate vice president and deputy general counsel for global, corporate, and regulatory affairs at Microsoft, where she had worked since 1996. And I have to say as a lawyer I am impressed by Microsoft's legal shop, particularly the really path-breaking work that they did to go after spammers and people who are coming after them on the Net with civil theories that dated back to probably 15th century English common law. It was quite impressive to see such ancient doctrines applied to such a new problem, and I think the Microsoft complaints in that area have really set a model not only for the rest of the corporate sector in that area of law but even for government enforcement in that area of law. So you come from a good place, and welcome.

STATEMENT OF PAMELA PASSMAN, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CENTER FOR RESPONSIBLE ENTERPRISE & TRADE (CREATE.ORG), WASHINGTON, DC

Ms. PASSMAN. Thank you very much, Chairman Whitehouse. Again, my name is Pamela Passman, and I am the CEO of the Center for Responsible Enterprise & Trade, CREATe.org. I appreciate the opportunity to testify.

CREATe is a nonprofit dedicated to helping companies reduce corruption and intellectual property theft, including trade secret theft. We provide resources to companies large and small that help them assess their risks and develop strategies to protect their trade secrets and other IP assets, both within their organizations and in their supply chains.

In today's integrated, global economy, companies that succeed in turning their knowledge and know-how into competitive advantage are the ones that will create new jobs and drive economic growth.

Increasingly, companies rely on trade secret laws to protect this knowledge. Yet the tremendous value of trade secrets also makes them prime targets for theft.

CREATe recently teamed up with PricewaterhouseCoopers to assess the economic impact of trade secret theft and devise a framework for companies to mitigate threats. A copy of the CREATe-PwC report is attached to my written testimony.

The report makes clear that the problem of trade secret theft is massive and inflicts material damage on the U.S. and other economies. If we are to energize our economy by enabling innovative companies to protect their trade secrets, we need to focus on two key goals.

First, we need to incentivize companies to take proactive measures and implement best practices to secure their trade secrets on the front end, both within their own organizations and in their supply chains.

Second, we need a consistent, predictable, and harmonized legal system to provide effective remedies when a trade secret theft has occurred. Trade secret theft occurs through many avenues, and companies need different tools and strategies to protect against each type of threat actor.

Businesses need to be particularly cognizant of risks that arise in their supply chains. The growth in recent years of extended global supply chains, comprising hundreds or even thousands of suppliers, has brought tremendous benefits and given many firms an enormous competitive edge. But companies using extended supply chains often must share confidential and highly valuable business information with their suppliers, which may be located in a different country with different laws and different corporate norms.

In the face of this reality, it is absolutely essential that companies implement effective strategies to protect trade secrets not just within their own four walls, but with their suppliers as well. In the CREATe-PwC report, we recommend a five-step approach for safeguarding trade secrets and mitigating potential threats.

We suggest that companies, one, identify and categorize their trade secrets; two, conduct a risk assessment; three, identify the most valuable trade secrets to their operations; four, assess the economic impact of losing those secrets; and, five, use the data collected to allocate resources and strengthen existing processes for protection.

CREATe recently completed a pilot program with more than 60 companies in countries around the world that helped them assess vulnerabilities and implement procedures to mitigate threats.

Based on that pilot program, we just launched "CREATe Leading Practices," a service designed to help companies improve and mature their management systems for IP protection and for anticorruption.

Unfortunately, no amount of protection can completely safeguard all trade secrets from theft. Companies also need a legal system that provides predictable enforcement and meaningful remedies against bad actors.

Recent high-profile criminal enforcement actions are promising, and I applaud you, Chairman Whitehouse and Ranking Member Graham, for your focus on law enforcement. I am also encouraged by the efforts of Senators Coons and Hatch to create a harmonized system for owners of trade secrets that will serve as a model around the world.

The problem of theft that happens entirely overseas, highlighted by Senator Flake's legislation, is worthy of further study. Governments and companies both play a role in improving protection for trade secrets. In our view, companies would benefit from taking a more proactive role in assessing vulnerabilities and employing best practices to manage their risks. They also need an effective legal system through which to enforce their rights when their know-how has been misappropriated.

Thank you for holding this hearing and for giving me the opportunity to testify. I look forward to your questions. Thank you.

[The prepared statement of Ms. Passman appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you, Ms. Passman.

Our next witness is Drew Greenblatt, who is the president of Marlin Steel Wire Products in Baltimore. He has owned it since 1998. The company exports baskets and sheet metal fabrications to 36 countries and has been recognized as one of the 5,000 fastest-growing companies in the United States for each of the last two

years. Mr. Greenblatt serves as an executive board member of the National Association of Manufacturers and as chairman of the boards of both the National Alliance for Jobs and Innovation and of the Regional Manufacturing Institute of Maryland. He is also a member of the Maryland Commission on Manufacturing Competitiveness as well as the Governor's International Advisory Council.

We welcome you here, Mr. Greenblatt. Please proceed.

STATEMENT OF DREW GREENBLATT, PRESIDENT AND OWNER, MARLIN STEEL WIRE PRODUCTS, BALTIMORE, MARYLAND

Mr. GREENBLATT. Thank you, Chairman Whitehouse, Senator Hatch, Members of the Subcommittee on Crime and Terrorism. Thank you for the focus on this critical challenge of trade secret theft and the opportunity to testify today.

As you mentioned, my name is Drew Greenblatt. I am the president of Marlin Steel. We are based in Baltimore City. We are a leading manufacturer of custom wire baskets, wire forms, and precision sheet metal fabrications. We make everything in the USA. I am very proud to report that we also export to 36 countries, and my favorite country that we export to is China. We cater to the automotive, the medical, and pharmaceutical industries.

I am here for three reasons.

Number one, trade secrets are important not just for manufacturers that are big but also for small manufacturers like myself.

Number two, America's trade secret laws and policies must keep pace with today's threats, which increasingly are not only interstate but are international threats.

Number three, manufacturers need your help to effectively and efficiently protect and enforce trade secrets. We need to secure strong commitments in our trade agreements.

Like so many other manufacturers, Marlin Steel competes in a global economy. We succeed through investing in ideas and innovations and the hard work of our dedicated employees. When I bought Marlin in 1998, we were a local business, and we made commodity bagel baskets—18 employees, $800,000 a year in sales. Last year we almost hit $5 million in sales, and we now have over 24 employees.

We are a proud member of the National Association of Manufacturers. We average about 40 employees in the National Association of Manufacturers, and we have 12,000 members. I am also the cofounder and chairman of the National Alliance for Jobs and Innovation. We have 380 members.

Both NAM and NAJI are working hard to strengthen protection of trade secrets and intellectual property rights. We want to level the playing field for manufacturers and businesses throughout the United States.

Trade secrets are more important than ever. They include things like drawings, proprietary manufacturing processes, software, formulas. All of these things are very valuable to the Nation—$5 trillion for public companies and even more when you include small companies.

Small companies, our secret sauce is those trade secrets. That is our intellectual property. We leverage the expertise of our employees. At Marlin 20 percent of them are degreed mechanical engi-

neers. They come up with specific client performance characteristics for our baskets that make us unique and different than our Chinese competitors.

Some people think that almost three percent of our GDP is lost to these trade secrets being stolen. In our grandparents' day, trade secrets were stolen by individuals who were across town that would steal some of the customer lists. Now it could be done on a thumb drive, and it could be sold to governments or Chinese companies across the world.

These cyber incursions are very threatening to us. We have lasers in our factory, robots. If they could hack into our system, they could manipulate our equipment possibly and hurt our employees. That would be devastating to us. The thing I am most proud about is we have gone over 1,981 days without a safety incident. If some Chinese hacker or some foreign national were to be able to break into our system and manipulate our system, they could hurt our team.

We are doing everything we can to harden our network. We spent so much money hardening our network that we could hire another unemployed steel worker to fill that job rather than spending all this money on these activities.

The good news is Washington is starting to recognize this problem. We need Washington to do three things.

First of all, we need you to have strong operational collaboration between the Federal agencies. We cannot have the silo approach we have right now. We need the FBI cooperating with the Justice Department, cooperating with Customs, cooperating with TSA. We all have to work together.

Number two, we need access to Federal civil enforcement for trade secrets theft, well-conceived legislation like the *Defend Trade Secrets Act* recently introduced by Senator Coons and Senator Hatch. This is going to give us the ability to pursue people on the Federal level, not on the State level.

Finally, we need to meet the global challenge of trade secret theft with global solutions, good trade agreements to stop these thefts.

In conclusion, Chairman Whitehouse, Senator Hatch, trade secrets are vital for manufacturers small and large. America's trade secret laws and policies much keep pace with today's threats. Manufacturers need your help to ensure that they can effectively and efficiently protect and enforce their trade secrets.

I applaud your attention to this critical challenge and your focus on solutions. With strong global partnerships and closer collaboration between Federal agencies and between government and business, and with the improvements to these U.S. laws, including Federal civil enforcement, we can have a real impact. We desperately need it now.

Thank you for the opportunity to testify this afternoon. I look forward to answering your questions. Thank you.

[The prepared statement of Mr. Greenblatt appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you, Mr. Greenblatt.

Our final witness is Douglas Norman, the vice president and general patent counsel for Eli Lilly and Company. He serves as a member of the Board of Intellectual Property Owners Association

and as Chair of the National Association of Manufacturers' Subcommittee for Intellectual Property. Mr. Norman has previously served as the 2002 co-chair of the Intellectual Property and Antitrust Task Force for the United States Council for International Business.

Welcome, Mr. Norman. Please proceed.

STATEMENT OF DOUGLAS K. NORMAN, VICE PRESIDENT AND GENERAL PATENT COUNSEL, ELI LILLY AND COMPANY, INDIANAPOLIS, INDIANA

Mr. NORMAN. Good afternoon, Chairman Whitehouse, Mr. Hatch, and other Members of the Subcommittee. Thank you for the opportunity to testify today on an issue of great importance not only to my company—and not only to my industry—but to all segments of the American economy.

Eli Lilly and Company was founded and is headquartered in Indianapolis, Indiana. On May 10th, just last Saturday, Lilly celebrated its 138th birthday as a U.S. company. Our mission at Lilly is to discover and develop medicines that help people live longer, healthier, and more active lives. Our major areas of innovation include therapies for cancer, diabetes, and mental illnesses. To fulfill this vision, Lilly must rely upon intellectual property protection that includes patents, trademarks, and trade secrets. Unfortunately, like too many of America's leading innovator firms, Lilly has recently been the victim of trade secret theft.

Lilly is a member of the Protect Trade Secrets Coalition, a cross-sector group of companies that supports a harmonized Federal civil remedy for trade secret misappropriation. We are pleased to support the *Defend Trade Secrets Act*, S. 2267, which would accomplish this objective. We thank Senators Coons and Hatch for their leadership. And we are also encouraged by your work, Chairman Whitehouse and Ranking Member Graham, to ensure law enforcement has the tools it needs to prosecute trade secret theft. And we appreciate the effort by Senator Flake to highlight the continued problem of trade secret theft that occurs abroad.

The bipartisan interest in trade secret protection evidenced by this Committee's work is important to our shared objective of improving the effectiveness and efficiency of remedies against trade secret misappropriation.

Trade secrets are an essential form of intellectual property and part of the backbone of our information-based economy. Whether you are a major pharmaceutical firm like Eli Lilly or a startup software company, your trade secrets are a big part of what sets you apart in the marketplace, and their protection is vitally important to maintaining a competitive edge and keeping workers on the job.

Unfortunately, companies that are creating jobs in America are increasingly the targets of sophisticated efforts to steal proprietary information, harming our global competitiveness.

Trade secrets are particularly vulnerable to theft given the rise in global supply chains and the rapid technological advances that have resulted in greater connectivity. A theft can come through cyber attack, voluntary or involuntary disclosure by an employee or by a joint venture partner.

The *Economic Espionage Act* makes the theft of trade secrets a Federal crime, and an array of State laws provide civil relief. The tools thieves use in their attempts to steal American trade secrets are growing more sophisticated by the day, however. Our laws must keep pace.

The EEA as a criminal statute necessarily has limitations, but we very much appreciate the cooperation we get from Federal law enforcement. The FBI and the Department of Justice have limited resources at the time and would never be in a position to bring charges in all cases of interstate trade secret theft. State laws provide an important right for trade secret owners to bring a civil action for relief.

State trade secret laws developed and made sense at a time when misappropriation was largely a local matter. But for companies that operate across State lines and have their trade secrets threatened by competitors around the globe, the array of State laws is inefficient and often inadequate.

It is also inconsistent with how other forms of intellectual property are protected. Trade secret theft today is increasingly likely to involve the movement of the secret across State lines and require swift action by courts to preserve evidence that protect the trade secret from being divulged. This is particularly true when the theft is by an individual looking to flee the country.

Once the trade secret has been divulged or is made known to a competitor, trade secret protection may be lost forever, and the harm from disclosure is very often irreparable.

We are pleased that the *Defend Trade Secrets Act* would address these limitations and provide trade secret owners with the same ability to enforce their rights in Federal court as owners of other forms of intellectual property have.

The breadth of support for the legislation—from companies focused on diverse areas such as software, biotechnology, semiconductors, medical devices, agriculture, and apparel—demonstrates the importance of a harmonized, Federal civil remedy. The companies that have already indicated their support for S. 2267 often disagree on other areas of intellectual property protection, but we are united on this front.

We also look forward to working with Chairman Whitehouse and Ranking Member Graham on ensuring law enforcement has the tools it needs to prosecute trade secret theft. Similarly, we look forward to working with Senator Flake and agree that it is important to study ways in which we can address overseas theft effectively.

In conclusion, American companies are competing globally, and our know-how is subject to theft everywhere. A national solution that provides consistent and predictable trade secret protection and enforcement is, therefore, essential to our global competitiveness. The *Defend Trade Secrets Act* will establish the gold standard for national trade secret laws globally and serve as an important base for international harmonization efforts. We urge the Committee to consider this legislation and for all Senators to support it.

Thank you again for the opportunity to testify today. I look forward to your questions.

[The prepared statement of Mr. Norman appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you, Mr. Norman.

Let me welcome Senator Hatch and Senator Coons to the hearing, and before I turn to them for their questions, let me ask unanimous consent that Chairman Leahy's statement be put into the record, which it will be without objection.

[The prepared statement of Chairman Leahy appears as a submission for the record.]

Chairman WHITEHOUSE. Let me ask each of you just very simply and quickly, using your own words and your own experience, explain what you think the scope is of this problem for our country and its industries, starting with Mr. Hoffman.

Mr. HOFFMAN. It is a tremendously big problem for us as a company, and, I think, more broadly as an industry because so much of our intellectual property is protected as trade secrets. And right now, a lot of those are very vulnerable considering the changing landscape, the sophistication of the means by which our intellectual property and trade secrets can be obtained. So anything that helps to improve law enforcement's ability to protect our trade secrets and allows us to be more secure in keeping those secrets so they are still valuable is very much appreciated by Boeing.

Chairman WHITEHOUSE. Ms. Passman, from your experience the scope of the problem.

Ms. PASSMAN. Well, with companies having almost 75 percent of their value in intangible assets like intellectual property, including trade secrets, the problem is quite significant. In the CREATe-PwC report, we attempted to put a figure to the magnitude of the problem, looking at the different threat actors that are involved, looking at the fact that U.S. companies, other advanced economies rely on distributed supply chains increasingly, and we looked at other illicit economic activity as a proxy for this, since it is a figure that is very difficult to get one's arms around because companies themselves do not know the magnitude of the trade secrets they have as well as when there is a trade secret theft.

We looked at other examples of illicit activity—corruption, money laundering, similar kinds of threat actors—and came to a figure of one to three percent of GDP. Quite significant.

Chairman WHITEHOUSE. Thank you.

Mr. Greenblatt, in your experience.

Mr. GREENBLATT. This problem is out of control. We need your help. We are being attacked daily. What this will have, if we can get this legislation enacted, this will save jobs. In Baltimore City, unemployed steel workers will be employed. We are getting things stolen left and right. We need your help.

Chairman WHITEHOUSE. And, Mr. Norman? Top that for clarity, by the way.

[Laughter.]

Mr. NORMAN. I will try to add some clarity myself.

The issue is enormous. I could speak on behalf of pharmaceutical firms that spend billions of dollars every year doing research and development. As we move forward and try to develop new life-saving medicines, we continually build chemical platforms and pharmaceutical platforms in hopes of reaching a point where we can apply for patents.

What we are seeing are numerous instances where interlopers are stepping in and trying to steal our trade secrets on our formula prior to the time we can reduce those into a patent application. It very often may take two or three years or longer to do enough research to get to the single molecule that we think will be able to be carried on into clinical trials.

If we lose the trade secrets and all of that formula prior to the time we can reduce that to a patent application, the loss is irrevocable. So we may spent $10, $20, $30 million building a chemical platform, a rich diversity of a number of compounds, and if any one of those is stolen from us prior to the time that we can obtain a patent on it, then it is lost forever. And, therefore, the public—no citizen gets the ability to enjoy the fruits of that research once it is gone.

Chairman WHITEHOUSE. Thank you very much.

Senator Hatch.

Senator HATCH. Thank you, Mr. Chairman.

Chairman WHITEHOUSE. And I should say both to you and Senator Coons that before you got here, your names were sung with praise over and over again for the legislation. It was almost as if you were summoned here by those voices.

Senator HATCH. That is always unusual.

[Laughter.]

Senator HATCH. We are happy to have all of you here. You are all experts in your field, and let me just ask Mr. Norman and Mr. Hoffman to respond to this one. Under U.S. law, protections for trade secrets are already some of the most robust in the world, and we are hoping to make those protections even stronger. But protecting trade secrets in numerous countries is a challenge, it seems to me, facing many transnational companies, something I am very concerned about.

Now, Mr. Norman and Mr. Hoffman, how will changes we make to U.S. law have an impact, either positive or negative, on what other countries are doing in this area? And do we need to be careful here? Mr. Norman, you can go first.

Mr. NORMAN. Sure. Thank you again, Senator Hatch, for the legislation that you have introduced. We greatly appreciate it. We greatly appreciate your leadership.

The instances of what it would do on a positive standpoint is that we believe the legislation to obtain a Federal trade secret remedy, particularly the ability to seek an ex parte seizure of stolen materials and prevent further disclosure or divestment of that information broadly, would be a very positive gold standard for future discussions on harmonization of trade secret laws around the world with our major trading partners.

It is important, I believe, to get beyond the State trade secrets laws, which are often a bit unwieldy and difficult to enforce across State lines simply because the procedures are not always set up to work very well along those lines. But with a Federal standard, with the appropriate kind of ex parte control, I believe we can show the rest of the world what the gold standard would look like as far as giving us the rights on our own to take a private civil action and protect our trade secrets.

Senator HATCH. Well, thank you.

Mr. NORMAN. Thank you.

Senator HATCH. Mr. Hoffman, do you care to add anything?

Mr. HOFFMAN. Yes. I fully agree with my colleague. Any opportunity for our trade negotiators to be able to point to improvements in trade secret laws in the United States to help strengthen the laws outside of our borders, for global companies such as ours, will be very helpful to protecting our trade secrets.

Senator HATCH. Okay. Let me ask a question for the whole panel, and that is, trade secrets also seem to be a lot more difficult to protect than patents. I understand that there may be industry best practices and model policies, but I imagine that these vary widely based on the industry and type of process or information that you are trying to protect. So I am very interested in, as a practical matter, how do you determine what measures are reasonable to protect your trade secrets. Mr. Hoffman.

Mr. HOFFMAN. Well, when it comes to trade secret versus patent, we actually base that decision upon the reverse engineering ability of the innovation. But once we decide to go the trade secret route, we have to have the processes and the systems in place in order to assure that those trade secrets are secure. And as mentioned previously, 60 percent of what we sell we buy from others, so the sharing of our intellectual property across our supply chain domestically and internationally is an area we are going to have to be very careful that they have the same type of procedures in place that will protect our intellectual property at the same level.

Senator HATCH. Okay. Yes.

Ms. PASSMAN. In our work with companies around the world, we have found that this is something that is not very mature inside their businesses or with their supply-chain partners. So in the CREATe work with PwC, we laid out a five-step framework for companies to begin to get their arms around how to best manage their intellectual property. And, really, first being able to identify and categorize what you have and where it is in a company is critical, whether you are a small company or a large company that has global operations.

We also recommend that companies conduct a risk assessment and identify who are the primary threat actors, who is interested in their trade secrets, in their intellectual property, and their potential vulnerabilities in their policies, in their procedures, in their internal controls, really looking inside of their company and in their supply chain; and also identify those trade secrets that would have the greatest impact on the company's operations and business; also looking at the economic impact of a loss of a trade secret, understanding the magnitude that that will have on their business; and, finally, taking all of this information and allocating resources to better protect your trade secrets, thinking of it as an investment, not just a cost.

Senator HATCH. My time is up, Mr. Chairman.

Chairman WHITEHOUSE. Senator Coons.

Senator COONS. Thank you, Senator Whitehouse. I would like to thank you for chairing this hearing and for the great work that you and Senator Graham have done to make sure that we protect America's intellectual property.

We have heard from an array of witnesses today the compelling picture of what is really at stake here: Up to $5 trillion of value held in America's intellectual property and, in particular, in the form of trade secrets. We have criminal law prosecutions for the protection of trade secret theft. The *Economic Espionage Act* is a good platform, a good beginning. But as we have heard from you today as witnesses, there are significant gaps, and I applaud the Chair today, Senator Whitehouse, and Senator Graham for their hard work in improving efforts to deal with that.

The Department of Justice has many priorities and limited resources, and so it is unsurprising to me that there were just 25 trade secret cases brought last year. Before he leaves, I need to say my profound personal thanks to Senator Hatch for being a great partner and a good leader on this issue.

Senator HATCH. Well, same here. This young man has really done a very good job on this, and we hope we can get this through for you.

Chairman WHITEHOUSE. You even got a "young man" out of it.

[Laughter.]

Senator HATCH. I should refer to you as one, too.

Senator COONS. As a former intern for this Committee, I will say that I never imagined there would be a day when Senator Hatch would be patting me on the shoulder and saying, "I look forward to passing a bill with this nice young man."

[Laughter.]

Senator COONS. When at the time I was mostly passing cups of coffee.

It is a tremendous sense of satisfaction that I have gotten through working with Senator Hatch and with Eli Lilly and a number of other companies represented here today, and I am grateful to the National Association of Manufacturers and the Coalition for the Protection of Trade Secrets, and the Protect Trade Secrets Coalition for their very able and valued input as we have crafted this bill and tried to get to a place that makes sense, and that can help stem the gap in U.S. law to ensure that we really vigorously defend trade secrets.

Let me ask a series of questions quickly of the panel, if I might, before I run out of time. First, if I might, Mr. Hoffman, Boeing does business globally, as your testimony thoroughly demonstrates. Most of the significant threats to U.S. trade secrets today originate from other countries around the world. Can you speak to how respect for trade secret theft varies around the world and how our laws domestically and what we might enact in terms of measures to strengthen our domestic laws could then influence the protection of U.S. IP internationally?

Mr. HOFFMAN. I would be glad to, and thank you for the question, Senator Coons.

When you look at trade secret theft, regardless of whether it is coming from domestic or international threats, it hurts Boeing and it hurts other companies. But I think the best thing we can do as a country is to set the standard and provide the tools necessary for efficient and effective protection of our trade secrets and give those standards to our trade negotiators to press the issue with our counterparts.

Senator COONS. I could not agree more, and I appreciate that response.

If I might, Mr. Greenblatt, for Marlin Steel, an admirable small manufacturer that has grown significantly under your leadership, trade secret theft can impose an existential threat. If a thief succeeds in stealing, as you put it, your secret sauce, it can literally mean the end of the business in your case, very harmful to Eli Lilly or Boeing or Microsoft or others, but for a firm like Marlin Steel, a loss of trade secrets could literally mean the end. And securing your trade secrets and then asserting your rights in court can also be significantly expensive relative to the size of your business, and I saw this in my own experience as in-house counsel for a manufacturing firm.

Can you speak to how the existence of a Federal private right of action would reduce the cost of protecting your trade secrets and how having one uniform Federal standard might strengthen your ability to go after those who would steal your trade secrets?

Mr. GREENBLATT. The *Defend Trade Secrets Act* is very well crafted. It is going to help us go around the State system, which is very inefficient, it is very slow, and it is very expensive. Little companies cannot afford having lawyers in five different States on retainers trying to go after a bad actor. It would be much more elegant if we could have a Federal jurisdiction on this matter. It would be much more efficient. The Coons-Hatch bill, your bill, would tremendously accelerate our ability to stop bad actors and get good results.

Senator COONS. Thank you. If I might, Mr. Chairman, one last question of Mr. Norman.

Mr. Norman, just thank you again for your hard work and leadership, and in particular, one of the sections we worked on was the ex parte injunctive relief. If you would, explain why an authority like that is particularly important to Eli Lilly or to other companies facing trade secret theft.

Mr. NORMAN. Yes, sir. We often run into situations where we find that an ex-employee has left and is going to work for a competitor, and we find out something such that once they turn in their Lilly-issued computer, there has been a download of a number of documents which contain highly confidential Lilly trade secrets. These occurrences almost always happen on a late Friday afternoon, and, therefore, the best part, I believe, about the ex parte seizure aspect of the bill that is currently pending is the fact that we could go to Federal court and in one action kick out an ounce of prevention rather than worrying about a pound of cure a week or two later, when we can get the Indiana State courts involved or the New Jersey State courts involved or perhaps both the Indiana and New Jersey State courts involved, leading to a whole lot more expense if we have to go through State court, a whole lot more risk because we may not be able to isolate and seize the stolen materials as quickly; and, therefore, a Federal cause of action where we can go to a single court and institute the power of the Federal court system to seize stolen materials would be extraordinarily helpful in those situations. And I thank you for your leadership on this bill.

Senator COONS. Well, thank you, Mr. Norman. And, Ms. Passman, for your estimate, if my math is right, that is $150 to $450 billion a year, trade secret theft is a big deal. Senator Whitehouse, Senator Graham, your leadership in strengthening the criminal law protections for American companies is admirable, and I very much look forward to working with you to pass these two bills in tandem in a way that can strengthen the differences for the inventions and innovations of millions of Americans and thousands of companies.

Thank you, Senator.

Chairman WHITEHOUSE. Thank you.

And now our distinguished Ranking Member, Lindsey Graham.

Senator GRAHAM. Thank you, Mr. Chairman.

We seem to have two challenges: Protecting the Nation against what I think is an inevitable cyber attack on a large scale that is coming. The question is: Will we do something about it in time to diminish the effect? That is one problem the Nation faces from criminal terrorist enterprises and potentially nation states.

The other is the private sector trying to do business in a very interconnected, complicated world, and one of the things that America always has had going for her is that we are pretty innovative and we are always thinking outside the box, and other people are pretty good at copying.

From a criminal point of view, we are trying to put teeth into this area of the law. Mr. Hoffman, when you are overseas representing Boeing or trying to do a joint venture, what do you worry about the most? Some countries require you to have a 51-percent partner. Is that correct?

Mr. HOFFMAN. It varies by country, but in some cases you can have a majority share—in some cases you can have a minority share.

Senator GRAHAM. But you will have a forced partnership based on the host country's laws.

Mr. HOFFMAN. Whatever the laws are, it typically is some type of partnership, yes.

Senator GRAHAM. Okay. Well, these partnerships are created by the host country, not at your own choosing. I guess you can choose who to partner with, but to do business in that country, you have got to have a local partner, for lack of a better term.

Mr. HOFFMAN. In general, yes, sir.

Senator GRAHAM. How does the private sector and the Government interact when there is a trade secret theft or intellectual property theft in a foreign country? What more can we do? And how does that system work?

Mr. HOFFMAN. I am not an expert in those areas, but I can tell you that we are a very globally spread company, and when we make the decision to go into a country and do business, we study the laws and how we need to establish ourselves as a business and are prepared to defend our trade secrets as best we can, knowing that it is going to be a very different environment than we have here at home, in some cases.

Senator GRAHAM. Mr. Norman, when you do business overseas and you have a local partner, what is your biggest concern?

Mr. NORMAN. The biggest concern, of course, is losing our trade secrets, losing the value of all the investment that we put in——

Senator GRAHAM. Having a company across the street from where you locate doing exactly the same thing you are doing?

Mr. NORMAN. Right. That is always an issue, and, therefore, we are quite circumspect about the type of research, development, or disclosure that we make in many of the partnered institutions where we do business outside the United States.

Senator GRAHAM. And if we had laws on our books that would hold a country or an individual acting on behalf of a nation state liable for engaging in that kind of theft, do you think it would make doing business easier overseas?

Mr. NORMAN. I believe it would, if we can use that as the standard by which we can get other countries to change their laws and more harmonize them with the appropriate way that we would like to see trade secrets protected, yes.

Senator GRAHAM. Mr. Hoffman, is it fair to say that in the international arena, when it comes to protecting intellectual property, trade secrets, in many countries it is the "Wild, Wild West"?

Mr. HOFFMAN. There is definitely different threat levels out there, and I agree with my colleagues that we choose carefully about what type of work and what type of intellectual property we do outside the United States.

Senator GRAHAM. And the more we could get this right, the more opportunity to create jobs here at home and abroad. Is this an impediment to job creation?

Mr. NORMAN. I believe any time we lose the fruits of the labors that our scientists and engineers put into developing drug products, it is a huge jobs issue. We employ thousands of scientists and engineers who will work years trying to develop a drug product, and if a competitor can step in and take that away from us right before we cross the finish line, it is devastating.

Senator GRAHAM. Well, I just want to thank Chairman Whitehouse. I have never known anyone more knowledgeable about the subject matter and who had a real zeal to do something about it, so I look forward to seeing if we can get our bill over the finish line here.

Chairman WHITEHOUSE. It has been a pleasure working with Senator Graham on a variety of cyber issues, and I thank him for his leadership.

Senator Flake, the floor is yours.

Senator FLAKE. Thank you, Mr. Chairman. And thank you for being here. I apologize for not being here earlier, and I hope I am not plowing old ground here.

But I am concerned about the rate at which trade secrets are being stolen, internationally on a foreign basis as opposed to domestically, and let me get some sense of that. I have introduced legislation, the *Future of America Innovation and Research Act*, the FAIR Act, which allows the owner of a trade secret to bring civil action in Federal court against the person who stole the trade secret if the bad actor is located abroad or acting on behalf of a foreign entity.

Ms. Passman, there was a recent report by CREATe.org that cited a survey of U.S. firms that were asked to report on suspected

successful or unsuccessful attempts to compromise trade secrets information. Of the incidents where the nationality of the primary beneficiary of the theft was known, 70 percent of the time it was foreign individuals, firms, or governments that were those beneficiaries.

Do you see this as a growing problem, the foreign nature of the threat?

Ms. PASSMAN. Well, certainly in an integrated economy with very distributed global supply chains, we are going to increasingly see the challenge with the trade secrets. You know, American companies benefit from having participated in these global supply chains, and as they move their business overseas, whether it is a supplier overseas or a customer overseas, they need to understand the global environment in which they are working.

We are working with companies around the world, including with companies in China and other emerging markets, that also want to mature their systems and better protect intellectual property.

But, you know, we advise companies to understand the environment that they are entering and to put business processes in place to better protect and manage their intellectual property inside of their business as well as with their supply chain.

Senator FLAKE. Well, thank you.

Mr. Hoffman, in your testimony you note that one of the few cases DOJ has prosecuted under Section 1831 was against a defendant who stole trade secrets from Boeing related to the Space Shuttle and the Delta IV rocket to benefit a foreign entity. Are you are also seeing an uptick in this foreign activity?

Mr. HOFFMAN. With that particular case, the gentleman was charged with stealing our trade secrets. There was no particular focus on what happened to those secrets. In fact, once a secret escapes, of course, the damage has been done. I might defer to our Department of Justice colleagues regarding those issues.

Senator FLAKE. All right. What is Boeing specifically doing to combat this? What measures have you taken? Sorry, again, if I am plowing old ground here.

Mr. HOFFMAN. In terms of our overseas presence, we hold our subsidiaries and our relationships with partners to the same level we have in the United States. The complexities are that we are in a different country and we have to adhere to their laws, and they may not be as harmonized with ours and as effective as ours.

Senator FLAKE. Do you think it is important to have legislation that protects companies against domestic and foreign trade secret theft? Do all of you agree with that? All right. Good. We will proceed with the legislation. I appreciate——

Chairman WHITEHOUSE. Everybody nodded, let the record reflect.

Senator FLAKE. Okay. If you could do that more audibly next time, that would be great.

Thank you for your testimony.

Chairman WHITEHOUSE. Let me ask one last, or maybe two last, questions of everybody.

There has been some reluctance on the part of corporate victims of trade secret theft to engage in the criminal law enforcement process, and one of the things that we have heard has been that taking that step rather than just simply trying to bury things could

actually make matters worse as the trade secret rattled around through the case and became more public and further compromised the company's secrecy and its advantage.

Is that something that is a real concern? Are there any other concerns that we should be looking at in terms of things having to do with the process of a criminal case that are deterring criminal victims from taking advantage of that means of redress? Mr. Norman.

Mr. NORMAN. Yes, Chairman Whitehouse, that is very much a deep concern that we have as we look at the question of criminal prosecution arising from a disclosure of trade secrets outside the bounds of our corporate entity. And I applaud you particularly for the language that you have in your legislation concerning the ability to protect a trade secret even during the time that the court is reviewing, because it is often difficult to question witnesses, it is very difficult to come forward with documentation, it is very difficult to seek expert testimony that can help prove that a theft has occurred if you cannot talk about specifically in open court what the means of the disclosure was or what the subject matter of the disclosure was. Because once it has made its way into open court, it is no longer a trade secret and you lose it anyway.

And so many of the mechanisms that have been proposed—and the mechanism in particular that I have seen in your legislation, I believe, is a great leap forward in helping us move into an arena where we could help prosecute these cases much more readily than we have been able to in the past, and I thank you for that.

Chairman WHITEHOUSE. A final question for Mr. Greenblatt. You indicated earlier that one of the things that we as Senators should focus on is improving coordination among the agencies. You used the term "silos." When I go out to the unofficially termed "fusion centers," if you will, where the FBI, for instance, leads one, or Homeland Security, they have got all the agencies there. They have got everybody represented. It is all up on screens. It looks like a model of interagency cooperation, at least at that level. Obviously, you had a different experience down at the level of the attacks on your company and the experience that you had. Could you articulate more specifically exactly what your concerns were about the silo problem and the problems of coordination?

Mr. GREENBLATT. So, for example, if we identify, if the FBI identifies a bad actor, we would like that that company cannot import things into America and the Customs agency halts their products from coming into America. The only way we are going to get their attention is by the wallet, and if we could stop them from shipping into the greatest, biggest economy in the world, we will get their attention.

Chairman WHITEHOUSE. Okay. So your experience was not that on the investigative side there was discoordination; rather, that when a case is done, you should be able to have as a remedy that the company does not get to import goods, it is an additional penalty for them?

Mr. GREENBLATT. Precisely. And we just want everybody to work together and quickly resolve these topics, and we just cannot have each agency in their own little zone. We have to have everybody working together and collaborate as much as possible. And then we

have to stop these bad actors from bringing their parts into America.

Chairman WHITEHOUSE. All right. Well, let me thank all of the witnesses for coming in. This is a very helpful process for us. We have a lot of things going for us with this legislation. For one thing, it is a real issue that is causing Americans to be hurt in very concrete and meaningful ways.

Second, as you have seen today, it could not be more bipartisan, so I do not see us getting dragged into the partisan turmoil. We are following regular order and having proper hearings and so forth so that we can pull this together and move it forward. But I hope very much that we will be able to make progress. And the advice and the counsel of all of you who are here, some of whom have been very helpful in the preparation of the legislation as well as in testimony about it, is something that we are all very grateful for. I think Senator Flake, Senator Hatch, Senator Coons, Senator Graham, and myself have all put considerable effort into trying to address different aspects of this problem, and I am confident that we will all continue to work together to try to solve this problem so that you have one less thing to worry about and you can focus your considerable skills on making the best products in the world and expanding your businesses.

Thank you very much. The hearing record will stay open for an additional week for anybody who wishes to add anything, but subject to that, we are adjourned.

[Whereupon, at 3:56 p.m., the Subcommittee was adjourned.]

APPENDIX

Additional Material Submitted for the Record

Witness List

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

On

"Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?"

Tuesday, May 13, 2014
Dirksen Senate Office Building, Room 226
2:30 p.m.

Panel I

Randall C. Coleman
Assistant Director, Counterintelligence Division
Federal Bureau of Investigation
Washington, DC

Panel II

Peter L. Hoffman
Vice President, Intellectual Property Management
The Boeing Company
Chicago, IL

Pamela Passman
President and Chief Executive Officer
Center for Responsible Enterprise And Trade
Washington, DC

Drew Greenblatt
President
Marlin Steel Wire Products
Baltimore, MD

Douglas K. Norman
Vice President and General Patent Counsel
Eli Lilly and Company
Indianapolis, IN

PREPARED STATEMENT OF CHAIRMAN PATRICK LEAHY

Statement of Senator Patrick Leahy
Chairman, Senate Judiciary Committee
Hearing on "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?"
May 13, 2014

Today, the subcommittee on crime and terrorism is examining the adequacy of our trade secret laws. This hearing raises a number of critical economic issues for American companies and consumers.

American businesses often choose to rely on trade secret protection over other forms of intellectual property protection, allowing them to shield commercially valuable information from their competitors. For that choice to remain viable, we must ensure that our laws protect trade secrets from theft and meaningfully deter and punish economic espionage. Today, American businesses face increasing threats both domestically and abroad from competitors that seek an advantage not through hard work, but through theft and deception.

The theft of trade secrets has also been linked to foreign governments in recent years, with countries seeking to undermine our national security and economy through theft of critical commercial information. While on a recent trip to China, I met with government officials to emphasize the need for strong global protection of trade secrets. I also met with Americans doing business in China and they stressed that theft of their trade secrets was a real threat to their livelihoods. As we continue to explore opportunities to work with other nations, we must emphasize this issue as a priority for American businesses and an area of ongoing focus for the United States.

The Administration has continued to apply diplomatic pressure abroad to curb trade secret theft and economic espionage, but there is also room for improvement domestically. We must be vigilant in ensuring that American companies can protect the products they work so hard to develop. Doing so will allow those companies to grow and thrive and protect critical American jobs.

Last Congress, we passed two laws that helped improve our trade secret policy, including the Theft of Trade Secrets Clarification Act that I introduced to close a troubling loophole in the law. I am pleased that this Committee is continuing its bipartisan work in this area. I look forward to working with Senators Whitehouse and Graham, Senators Coons and Hatch, and with all members of this Committee on this issue.

I thank Senator Whitehouse and Senator Graham for holding the hearing today and welcome the testimony of the witnesses.

#####

PREPARED STATEMENT OF CHAIRMAN SHELDON WHITEHOUSE

Senator Sheldon Whitehouse
"Economic Espionage and Trade Secret Theft:
Are Our Laws Adequate for Today's Threats?"
May 13, 2014
Opening Statement as Prepared for Delivery

Welcome to today's hearing entitled "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?" Today, this Subcommittee will explore how we can better protect American businesses from those who try to steal their valuable intellectual property.

American companies are the most innovative in the world. Companies of every size and in every industry – from manufacturing to software to biotechnology to aerospace – own large portfolios of legally protected trade secrets. In some cases, the "secret sauce" may be a company's most valuable asset. The theft of these secrets can lead to devastating consequences: for small businesses, it can be a matter of life and death.

The risk of trade secret theft has been around as long as there have been secrets to protect; there is a reason why Coca-Cola has kept its formula locked away in a vault for decades. But in recent years the methods used to steal trade secrets have become more sophisticated. Companies now must confront the reality that they are being attacked, on a daily basis, by cyber criminals who are determined to steal their intellectual property. As Attorney General Holder observed, there are two kinds of companies in America: "those that have been hacked, and those that don't know they have been hacked." Today, a criminal can steal all of the trade secrets a company owns from thousands of miles away without the company ever noticing.

Many of the cyber attacks we are seeing are the work of foreign governments. China and other nations now routinely steal from American businesses and give the secrets to their own companies. And let's be clear: we do not do the same to them. We are now going through a healthy debate about government surveillance, but there is no dispute about one thing: our spy agencies do not steal from foreign businesses to help American industry.

While cyber attacks are increasing, traditional threats remain. Company insiders walk off with trade secrets to sell to the highest bidder. Competitors steal secrets through trickery or by simply breaking into a factory or office building.

It is impossible to determine the full extent of the loss to American businesses as a result of the theft of trade secrets and other intellectual property. There have been estimates that our nation may lose anywhere from 1-3% of our GDP through trade secret theft alone. The Defense Department has said that, every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from computer networks belonging to American businesses and governments, and estimates of the value of IP stolen by foreign actors are as high as $300 billion. General Keith Alexander has characterized the cyber theft of American intellectual property as "the greatest transfer of wealth in history."

But no estimate can fully capture the real impact of trade secret theft. Because when other countries and foreign businesses steal our trade secrets, they are stealing our ideas. They are stealing our innovation. Most importantly, they are stealing our jobs.

In my own state of Rhode Island, we continue to face unacceptably high unemployment – despite having some of the most innovative businesses in the country. If we do not protect our

businesses from those who steal their intellectual property, then we are letting that innovation go to waste, and we are letting American jobs go overseas.

In the past, some companies were reluctant to talk about this issue, because no one likes to admit that they have been victimized. But many are coming forward to speak out now because they recognize how important it is that we work together to address this threat. I particularly want to thank the company representatives who are appearing before us today, as well as the many others who have working closely with me and other Senators.

I am encouraged that the Administration released a blueprint for a strategy to combat trade secret theft last year, and agencies across the government are increasing efforts to address this problem. The Administration must recognize that the theft of intellectual property is one of the most important foreign policy challenges we face, and it must communicate to China and other nations that stealing from our businesses is unacceptable.

We in Congress must do our part. We need to make sure that our criminal laws in this area are adequate and up to date. Last fall, Senator Graham and I released a discussion draft of legislation designed to clarify that state-sponsored overseas hacking could be prosecuted as economic espionage, and to strengthen criminal protection of trade secrets. We received valuable comments and suggestions about the legislation. We look forward to hearing from our witnesses today about how to improve our laws, and we hope to introduce our legislation in the coming weeks.

Companies also need civil remedies against those who steal from them. While state law has traditionally provided companies with remedies for misappropriation of trade secrets, there is currently no federal law that allows companies themselves to seek civil remedies against those who steal from them. Senators Coons and Hatch have recently introduced legislation to give victims of trade secret theft the option of pursuing thieves in federal court. Senator Flake has also introduced legislation to give companies a federal civil remedy for trade secret theft. I hope that the Judiciary Committee will act soon on legislation to strengthen both the criminal and civil protections against trade secret theft, and I look forward to working with my colleagues toward that goal.

Today, we will hear from witnesses in government, industry, and the nonprofit sector who confront the threat of trade secret theft on a daily basis. What I hope will be clear by the end of this hearing is that we need an "all-in" approach to this problem. We must strengthen our criminal laws, and our law enforcement agencies must prioritize stopping trade secret theft before it occurs and investigating and prosecuting it when it does. I will add that there remains an urgent need for us to pass broader cybersecurity legislation, and I appreciate working with Senator Graham on that effort.

I look forward to hearing from our witnesses today and to working with my colleagues on both sides of the aisle to address this critical issue.

PREPARED STATEMENT OF RANDALL C. COLEMAN

Department of Justice

STATEMENT OF

RANDALL C. COLEMAN
ASSISTANT DIRECTOR
COUNTERINTELLIGENCE DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME AND TERRORISM
UNITED STATES SENATE

AT A HEARING ENTITLED

"ECONOMIC ESPIONAGE AND TRADE SECRET THEFT: ARE OUR LAWS ADEQUATE FOR TODAY'S THREATS?"

PRESENTED
MAY 13, 2014

Randall C. Coleman
Assistant Director
Counterintelligence Division
Federal Bureau of Investigation
Statement Before the Senate Judiciary Subcommittee on Crime and Terrorism
Washington, D.C.
May 13, 2014

Good morning Chairman Whitehouse, Ranking Member Graham, and distinguished members of the subcommittee. I am pleased to be here with you today to discuss the Federal Bureau of Investigation's (FBI) efforts to combat economic espionage and trade secret theft.

Scope of the Problem

Theft of trade secrets occurs when someone knowingly steals or misappropriates a trade secret to the economic benefit of anyone other than the owner. Similarly, economic espionage occurs when a trade secret is stolen for the benefit of a foreign government, foreign instrumentality, or foreign agent. Both crimes are covered by the Economic Espionage Act of 1996, Title 18, Sections 1831 and 1832 of the U.S. Code.

U.S.-based businesses, academic institutions, cleared defense contractors, and government agencies are increasingly targeted for economic espionage and theft of trade secrets by foreign entities, often with state sponsorship and backing. The Office of the National Counterintelligence Executive, using estimates from academic literature, has estimated losses from economic espionage to be in the tens or even hundreds of billions of dollars annually to the American economy.

Our foreign adversaries and competitors are determined to acquire, steal, or transfer a broad range of trade secrets in which the United States maintains a definitive innovation advantage. This technological lead gives our nation a competitive advantage in today's globalized, knowledge-based economy. Protecting this competitive advantage is vital to our economic security and our national security. Trade secret theft has hit some of the nation's best-known companies, such as DuPont and Goodyear. To highlight one case in the news earlier this year, a federal jury convicted three defendants in the DuPont case, Walter Liew, Liew's company, USA Performance Technology Incorporated, and Robert J. Maegerle, of 20 charges, including economic espionage and theft of trade secrets. Liew and Maegerle stole trade secrets from DuPont and sold the information to state-owned companies in China.

Fighting economic espionage and theft of trade secrets from U.S.-based companies is a top priority of the FBI's Counterintelligence Division (CD). In 2010, CD created the Economic Espionage Unit, a specialized unit focused solely on prosecuting cases under the Economic Espionage Act. Located within CD's Counterespionage Section, the Economic Espionage Unit works with private sector partners to investigate and prosecute trade secret theft. Within CD, this unit's caseload has continued to

increase every year since its formation. In fact, from FY 2009 to the end of FY 2013, the number of economic espionage and theft of trade secrets cases overseen by the unit increased by more than 60 percent. Economic espionage and theft of trade secrets represent the largest growth area among the traditional espionage cases overseen by CD's Counterespionage Section.

Economic espionage and theft of trade secrets are increasingly linked to the insider threat and the growing threat of cyber-enabled trade secret theft. The employee who poses an insider threat may be stealing information for personal gain or may be serving as a spy to benefit another organization or country. Foreign competitors steal trade secrets by aggressively targeting and recruiting insiders; conducting economic intelligence through bribery, cyber intrusions, theft, and dumpster diving (in search of intellectual property or discarded prototypes); and establishing joint ventures with U.S. companies.

Long gone are the days when a spy needed physical access to a document to steal it, copy it, or photograph it where modern technology now enables global access and transmission instantaneously.

China often is cited as particularly active in the theft of trade secrets. According to a report submitted to Congress by the U.S.-China Economic and Security Review Commission in November 2012, China "depends on industrial espionage, forced technology transfers, and piracy and counterfeiting of foreign technology as part of a system of innovation mercantilism." [1]By obtaining what it needs illegally, China avoids the expense and difficulty of basic research and unique product development, the report concluded. Created by Congress in 2000, the Commission's mandate is to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China.

Enhanced Strategies for Law Enforcement

Officials across the U.S. Government are pursuing a comprehensive strategy to counter economic espionage as part of a larger campaign against intellectual property theft. In furtherance of this initiative, the U.S. Department of Justice (DOJ) formed a task force on intellectual property in February 2010. The task force works with the Office of the U.S. Intellectual Property Enforcement Coordinator (IPEC), located in the Executive Office of the President. In February 2013, IPEC issued the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets. The five part strategy calls for focusing diplomatic efforts to protect trade secrets overseas; promoting voluntary best practices by private industry to protect trade secrets; enhancing domestic law enforcement operations; improving domestic legislation; and raising public awareness and stakeholder outreach. The FBI is also a partner at the National Intellectual Property

[1] U.S.-China Economic and Security Review Commission, *2012 Report to Congress*, 112th Cong.,2d session (Washington, DC: Government Printing Office,2012):p.21.

Rights Coordination Center (IPR Center). Together the IPR Center's 21 partner agencies facilitate the exchange of IP theft information among federal government agencies and international partners, plan and coordinate joint domestic and international law enforcement operations, generate and deconflict investigative leads from industry and the public, provide law enforcement training and collaborate closely with industry partners on all forms of IP crime.

The DOJ has also taken steps specifically to address economic espionage. Our partners in DOJ's National Security Division (NSD), for example, are increasingly focused on deterring and disrupting these threats. The FBI works closely with NSD's Counterespionage Section (CES), whose leadership has deep experience and expertise in prosecuting economic espionage and related issues, and whose attorneys are, as the DuPont verdict shows, committed to prosecuting individuals and entities who commit and sponsor economic espionage by any means.

In addition, NSD, together with the Criminal Division, also established the National Security Cyber Specialists Network (NSCS) in 2012. This nationwide network of specially trained prosecutors who focus on cyber threats to the national security, including economic espionage, is actively working with the FBI to build cases against state sponsored cyber threat actors. The NSCS Network has also improved DOJ's outreach to the private sector on cybersecurity issues, including cyber-based economic espionage, both to help prevent intrusions and to improve the government's response when they occur.

FBI Outreach and Awareness Efforts

To raise public awareness and conduct stakeholder outreach, the FBI uses the Counterintelligence Strategic Partnership Program (CISPP) to mitigate the risks posed by foreign actors in illicitly acquiring sensitive technologies, advanced scientific research, classified USG information, and trade secrets from private industry and academia. The CISPP network consists of more than 80 special agents experienced in counterintelligence (CI) who are known as Strategic Partnership Coordinators (SPCs). The SPCs counter foreign intelligence threats to academia and private industry by conducting in-person classified and unclassified threat briefings. SPCs provide an early referral mechanism for reports of possible acts of economic espionage, theft of trade secrets, and cyber intrusions. Last fiscal year, SPCs conducted more than 7,500 presentations and briefings about these threats. At the national level, the CISPP manages the Business Alliance and Academic Alliance programs[2], which foster national and local partnerships between the FBI and private industry and academia.

[2] The Business Alliance and Academic Alliance programs develop partnerships with leaders from private industry and academia at the national level through the National Security Business Alliance Council (NSBAC) and the National Security Higher Education Advisory Board (NSHEAB). Both NSBAC and NSHEAB meet quarterly at FBI Headquarters.

SPCs currently maintain more than 15,000 contacts nationwide, consisting of local businesses, academic institutions, and cleared defense contractors. The CI threat briefings and intelligence products provided by SPCs on current trends and indicators help companies detect, deter, and defend against attacks to sensitive proprietary information from foreign adversaries.

This spring, the FBI released a new threat awareness film dramatizing the risks of economic espionage and theft of trade secrets to the American economy. Called *The Company Man: Protecting America's Secrets*, this 37-minute film is based on a trade secrets case recently investigated by the FBI. In the real-life case, a group of conspirators tried to recruit a veteran employee to steal the trade secrets they needed to build a competing plant in China. The film will raise the awareness of audiences about the threat of economic espionage and theft of trade secrets, and help organizations understand the indicators to watch for, so they proactively detect attempts by insiders and foreign agents to illicitly acquire trade secrets and intellectual property. These showings will also encourage viewers to report suspicious activity to the FBI, and help the SPCs build relationships with contacts in local industry and academia. Copies of *The Company Man* DVD have been shipped to the FBI's network of SPCs, who are showing the film and handing out educational materials during in-person screenings. The SPCs answer questions from audience members and are available for short discussions about economic espionage and theft of trade secrets afterwards.

Despite the comprehensive outreach efforts undertaken by the FBI, companies which discover misappropriation of their trade secrets, even misappropriation appearing to rise to the level of criminal trade secret theft, sometimes attempt to address the issue through private negotiations or civil litigation, rather than alert law enforcement. As one example of this problem, during a recent economic espionage investigation at a company, the FBI learned the company had been victimized previously on a separate occasion but pursued a civil action instead of contacting the FBI. The FBI is currently looking into whether this earlier incident involved criminal activity. The FBI is committed to ensuring companies have an established line of communication to report concerns about possible economic espionage or trade secret theft to law enforcement. But the FBI must assure companies the government will work to protect their proprietary information from disclosure during prosecution, so that more companies are willing to come forward and report concerns about possible trade secret theft.

Protecting the nation's economy from this threat is not something the FBI can accomplish on its own. To effectively protect trade secrets, companies need to be proactive—by marking sensitive material as secret or proprietary information, limiting access to protected material, and monitoring who accesses it. Employees should receive regular training, and more frequent notices regarding company policies on protecting trade secrets. Companies should consider implementing non-disclosure agreements with employees to not divulge company proprietary information. If a given piece of information is critical to the long-term success and profitability of a company, the company should limit access to those employees who have a need to know. Further, organizations and companies should evaluate internal operations and policies to

determine if current approaches are tailored to the types of risks and factors associated with trade secret misappropriation committed by corporate and state sponsors. For example, areas for evaluation might include: research and development compartmentalization, information and physical security policies, and human resource policies.

Companies also need to educate their employees about some of the warning signs of insider threat, and regularly explain how to report suspicious behavior. Some of these warning signs include working odd hours without authorization; taking home company proprietary information; and installing personal software, or personal media, on company equipment. Other warning signs include short trips to foreign countries without notification or for unexplained reasons, a sudden influx of wealth, or an employee living beyond his or her means. Companies need to get employees involved in protecting proprietary information and willing to come forward and report concerns about suspicious behavior. In many cases investigated by the FBI, co-workers don't report concerns until after an arrest.

FBI investigators should be contacted as soon as an insider threat is suspected to ensure the passage of time does not hinder any investigation that may be required.

Increased Penalties for Offenders

In 2011, the Administration recommended that Congress increase the statutory maximum sentence for economic espionage from 15 to 20 years. In addition, the Administration asked Congress to direct the U.S. Sentencing Commission to consider increasing the guideline range based on aggravated offense conduct in theft of trade secret and economic espionage cases. See Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations, March 2011, at 4-6 (available at http://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf).

In 2012, Congress responded to the growing threat of economic espionage by approving tougher penalties for those convicted of the crime with passage of the Foreign and Economic Espionage Penalty Enhancement Act of 2012. Formerly, an individual responsible for economic espionage faced a maximum fine of $500,000, and organizations faced a maximum fine of $10 million. Congress passed legislation boosting the maximum fine applicable to individuals to $5 million, and organizations responsible for committing economic espionage now face penalties of the greater of up to $10 million or up to three times the value of stolen trade secrets.

Congress also directed the U.S. Sentencing Commission to examine the sentencing guidelines for economic espionage and theft of trade secrets. Following public hearings in 2013, the Commission approved sentencing guideline enhancements where a trade secret is taken out of the country or where a defendant knows the trade secret will benefit a foreign government.

Challenges

Often, the greatest challenge in prosecuting economic espionage, as opposed to trade secret theft, is being able to prove that the theft was intended to benefit a foreign government or foreign instrumentality. The beneficiary of the stolen trade secrets may be traced to an overseas entity, but obtaining evidence that proves the entity's relationship with a foreign government can be difficult. The decision to pursue these cases under Section 1832 (theft of trade secrets) instead of Section 1831 (economic espionage) may depend upon the availability of foreign evidence and witnesses, diplomatic concerns, and the presence of classified or sensitive information required to prove the foreign nexus element. Since the law was passed in 1996, there have been 10 economic espionage convictions.

Conclusion

Theft of trade secrets and economic espionage is a significant and sustained threat to the nation's economy, and requires constant vigilance. The FBI is working to investigate, and apprehend targets pursuing economic espionage against the United States.

Thank you again for the opportunity to testify. I am now happy to answer any questions you may have.

PREPARED STATEMENT OF PETER L. HOFFMAN

Peter L. Hoffman
Vice President, Intellectual Property Management, The Boeing Company
Senate Judiciary Committee Subcommittee on Crime and Terrorism
"Economic Espionage and Trade Secret Theft:
Are Our Laws Adequate for Today's Threats?"
May 13, 2014

Introduction

Good morning, Chairman Whitehouse, Ranking Member Graham, and members of the Committee. On behalf of The Boeing Company, I thank you for convening this hearing and am grateful for your leadership on efforts to improve trade secrets laws. It is a privilege to be a participant on this panel and provide Boeing's view on the challenges faced by America's innovators.

Company Introduction

Boeing first began making twin-float seaplanes in 1915 from a small red boathouse in Seattle, and while much has changed since then, our company remains unique in that we assemble, test and deliver most of our highly-competitive products right here in the United States. The final assembly facilities for our commercial products are located in the states of Washington and South Carolina, but we have facilities for engineering and manufacturing major components in multiple states beyond those two—including Oregon, Florida, California, Montana and Utah, where we have a growing presence. Our defense and space-related production primarily is located in the states of California, Missouri, Pennsylvania, Texas, Arizona, Florida and Alabama.

Today Boeing has 160,000 employees across the United States. Both during and in the wake of the recent global recession we hired many new talent workers with critical skills—and created a total of more than 15,000 new, high-paying jobs since 2005. Our hiring has been driven by our record order backlog of $441 billion, $374 billion of that attributable to our commercial airplanes. With more than 5,000 commercial aircraft on order, our commercial backlog is diverse, with customers across the world committing to purchase a full range of Boeing airplanes. While 80 percent of our commercial airplanes go to airlines outside the United States, 80 percent of our supplier spend is with U.S. companies. Last year, we paid $48 billion to more than 15,600 U.S. businesses, including 6,600 small or disadvantaged businesses, which collectively support an additional 1.5 million jobs across the country.

Boeing's Trade Secrets Are Its Competitive Advantage

Boeing's significant contribution to the U.S. economy today, as it has been for the past 100 years, is the result of the ingenuity of our highly skilled workers. Innovating each step of the way, they develop the designs, drawings, software, chemical formulas and manufacturing techniques that make our commercial airplanes, fighters, transports, refueling aircraft, helicopters, satellites, electronic and defense systems, advanced information and communication systems—the most sought after products and technologies in the world. Boeing protects much of its intellectual property through trade secret laws.

Of course, Boeing's cutting edge technologies take years to develop at an enormous expense. For example, when we design, model, build, and test an airplane, even each component of a plane, we make tremendous investments of time and money. And we build several different kinds of planes. For each, Boeing invests in facilities, research and development, product design and production system design, implementation and, of course, countless hours of numerous teams of skilled engineers and technicians. But those investments can be wiped out in an instant. Once publicly disclosed, rights in trade secrets may be lost forever, along with the competitive advantage they provide. Boeing cannot afford to have its technologies stolen or have its competitors, both old and new, take advantage of decades of technology investment and the vast amount of spending Boeing has committed to perfect the design of just one of our products. But that is the real threat Boeing faces every day.

Trade secret protections are vital to protecting Boeing's substantial intellectual property. Boeing does not simply have one recipe for its secret sauce; Boeing has thousands of trade secrets that are critical to maintaining its unparalleled success. We not only invent new aircraft and techniques for building them, but we are constantly inventing and reinventing the thousands of components that go into them, and even the tools and processes for making those components. Unfortunately, Boeing's valuable scientific, technical, engineering, financial, business or economic information is at significant risk.

The Threat

Of course, Boeing is on constant guard to prevent the escape of our trade secrets. But today, companies cannot simply lock their trade secrets in a safe. The vast majority of our business and engineering information is stored electronically. And with the productivity that comes with the digital age also come significant risks. We recognize that at any moment we could lose a trade secret, through a breach of our network, through disclosure by one of our employees or partners, or through an escape at one of our or our many suppliers' facilities.

We know this because Boeing has been a victim of this crime. In a well known case, Boeing was victimized by an employee who collected sensitive documents containing trade secrets relating to technologies used in the Space Shuttle and Delta IV rocket programs.

We are not just up against mere thieves; in some cases, we are up against concerted public-private nation-state efforts using every collection platform at their disposal to aid their domestic industrial, military and economic development. To combat these sophisticated attacks requires truly innovative private-public partnerships that take advantage of information sources and talents within our federal organizations, as well as those skills contained within private industry. In addition to proactively working to protect our secrets, we need to tell those involved that this theft is a crime and send a message that we will not stand by as these concerted efforts harm our businesses, our economy and steal our jobs.

A Threat to the U.S. Economy

Fear of trade secret theft is not a concern just for Boeing. In February of 2013, the White House issued the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets ("White House Strategy"), which includes a summary of several criminal trade secret cases that the Department of Justice has prosecuted over the past few years. Targeted U.S. companies included an array of household names including Corning, DuPont, Motorola, Ford, GM, Dow Chemical, and many others. This summary details the theft, here in the United States, of the crown jewels of several major companies. Our partners at the Department of Justice can attest to the fact that if there are dozens of cases of trade secret thefts that have been publicly prosecuted, there are many more instances of theft which did not become public and were not addressed. The theft of these trade secrets enables competitors to move directly into the production of competing knock-off products, thereby avoiding the investments and risks that the U.S. innovator must shoulder to bring a product to market. And this is not just a concern for big businesses. Middle and small-size companies that rely on trade secrets have as much or more to fear as we do, particularly if their survival depends on a single product or service.

The White House Strategy concludes that the pace of economic espionage and trade secret theft against U.S. corporations is accelerating and moving to the cyber world. Because online attacks are hard to detect, allow access to more information at once, and are difficult to attribute, in its 2011 report, the Office of the National Counterintelligence Executive predicts that cyber intrusions will become the preferred

method for trade secret theft. Even though online trade secret theft appears to be on the rise, it is worth noting that none of the prosecuted cases listed in the summary of cases involved online theft.

The Need to Act

Given the risk U.S. companies face every day, something more needs to be done to deter cyber thieves from attempting to steal our trade secrets. Thus, we strongly support your efforts, Chairman Whitehouse and Ranking Member Graham, to call attention to the issue and to provide law enforcement with additional tools to help deter such trade secret theft. It is critical to the U.S. economy and necessary to protect jobs here that we take affirmative steps to strengthen our laws and further protect our invaluable trade secrets, and we are happy to help you in those efforts in any way we can.

We also applaud the efforts of law enforcement, both federal and state, to help companies react to the significant threat trade secret theft is to U.S. business and the U.S. economy. Undoubtedly, we have the best law enforcement in the world. I must emphasize that Boeing greatly appreciates the assistance it has received from law enforcement over the years. And while the Economic Espionage Act provides an excellent law enforcement tool to help stem the tide of this illegal activity, the threat is so pervasive that federal law enforcement cannot always be expected to go it alone.

While containing a vital trade secret may be the highest priority of a victim company, it would be unreasonable to expect it to always be the highest priority of federal law enforcement. Federal law enforcement is simultaneously combating significant crimes on many fronts. We acknowledge that its resources have limits. Thus, in addition to recognizing the need to strengthen law enforcement's authority to combat trade secret theft, we also acknowledge the need for companies to have the ability, in those cases when federal law enforcement cannot act swiftly, to take immediate action of our own to contain an escape of our trade secrets.

The Uniform Trade Secrets Act (UTSA) provides a general framework for state legislatures to adopt trade secret protections, and companies have successfully brought cases in state courts. As a model law, however, the standards, procedures and remedies can vary from state-to-state and the time needed for either state or company officials to come up to speed to adapt to local procedures may make all the difference. Jurisdictional issues may complicate matters further if, for example, the thief resides in a state different from the state in which the theft occurred. Accordingly, it is a real concern of U.S. companies that state action under the Uniform Trade Secrets Act may not, in some instance, be immediate enough to prevent the loss of a trade secret.

When a company has a trade secret on the verge of escaping its grasp, it must have the ability to act immediately to prevent that escape. Thus, we also applaud Senator Coons and Senator Hatch for introducing the Defend Trade Secrets Act and your efforts to establish the right for companies to file an application in a federal district court

requesting an order to seize property containing trade secrets stolen from the company, when necessary to prevent the irreparable harm disclosure of those trade secrets will cause. Stopping criminals from getting on a plane with our trade secrets and, thereby, preventing their disclosure, is indeed our highest priority. And, in those worst cases, where the secret is disclosed to a competitor and a company is seriously harmed, companies should be empowered to seek damages, so long as appropriate safeguards are in place to prevent abuse. We look forward to working with Senator Coons and Senator Hatch on this bill, and supporting your efforts to encourage the Congress to act quickly to pass this important legislation.

We are also thankful to Senator Flake for his recognition that many of these files are destined for competitors located outside of the U.S., and the difficulties U.S. companies face as a result. We are grateful for his efforts to address that aspect of the problem and look forward to working with Senator Flake to strengthen trade secret laws.

We are also encouraged that the new laws under discussion, if passed, would strengthen overseas trade secret enforcement, by raising awareness of the issue, promoting cooperation between U.S. and foreign law enforcement, and empowering our trade negotiators to encourage our trading partners to similarly raise the bar.

Closing

We applaud the efforts of Chairman Whitehouse, Ranking Member Graham and the other Members of the Subcommittee to highlight this issue and to strengthen U.S. trade

secret laws, and protect our most valuable asserts. Thank you for your time in hearing our concerns.

PREPARED STATEMENT OF PAMELA PASSMAN

Hearing on

"Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?"

United States Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

May 13, 2014

Statement of Pamela Passman
President and CEO
Center for Responsible Enterprise & Trade
(CREATe.org)

Testimony of Pamela Passman
President and CEO of CREATe.org
Hearing on "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?"
May 13, 2014

Good afternoon Chairman Whitehouse, Ranking Member Graham, and members of the Committee. My name is Pamela Passman, and I am the CEO of the Center for Responsible Enterprise & Trade, also known as CREATe. I appreciate the opportunity to testify here today about an issue that is vital to the economy and job growth.

CREATe is a nonprofit dedicated to helping companies reduce corruption and intellectual property theft, including theft of trade secrets. We provide resources to companies large and small that help them assess their risks and develop strategies to protect their trade secrets and other IP assets, both within their own organizations and in their supply chains.

In today's integrated, global economy, information and knowledge are the new crown jewels. Companies that succeed in turning their knowledge and know-how into competitive advantage are the ones that will create new jobs and drive our nation's growth.

Increasingly, companies rely on trade secret laws to protect this knowledge. A trade secret can be as simple as a customer list, or as complex as the know-how to manufacture microchips. In our work at CREATe, it has become apparent that trade secrets are critical to innovation, and by extension to investment and competitiveness.

Yet the tremendous value of trade secrets also makes them prime targets for theft.

Calculating the extent and impact of trade secret theft is notoriously difficult. Many companies do not keep good track of their trade secrets, and those that do often do not know when their property has been stolen. Even when they are aware, companies often are hesitant to disclose thefts that have occurred, for both reputational and other reasons.

CREATe recently teamed up with PricewaterhouseCoopers to assess the economic impact of trade secret theft and devise a framework for companies to mitigate threats. A copy of the CREATe-PwC report is attached to my written testimony.

In the report, we used several proxies for estimating the value of trade secrets and the harms caused by trade secret theft. For instance, we looked at data on other key forms of illicit activity, such as fraud and corruption, copyright theft, and various black-market activities. Based on these proxies and other data, we estimated that trade secret theft costs on average 1 to 3 percent of GDP in the United States and other advanced economies.

Whatever the exact number, the problem of trade secret theft is massive and inflicts material damage on the U.S. and other economies. If we are to energize our economy by enabling innovative companies to protect their trade secrets, we need to focus on two key goals:

- First, we need to incentivize companies to take proactive measures and implement best practices to secure their trade secrets on the front end, both within their own organizations and in their supply chains.

- Second, we need a consistent, predictable and harmonized legal system to provide effective remedies when a trade secret theft has occurred.

I am therefore greatly encouraged to see the bipartisan interest in exploring better and more efficient ways to protect trade secrets. By providing attention to this issue, Congress can motivate companies to adopt more effective processes for protecting their own trade secrets; focus law enforcement attention; and put the United States on a path to having a harmonized legal system that will serve as a model around the world.

While there is an important role for governments in protecting trade secrets—and I applaud, Chairman Whitehouse and Ranking Member Graham, your focus on law enforcement—companies also need to take the lead in more effectively protecting trade secrets within their companies and in their supply chains.

Trade secret theft occurs through many vectors, and understanding these vectors can help businesses assess internal vulnerabilities that they can prioritize for fixing. Cybercrime is one clear avenue through which bad actors steal trade secrets, and I welcome this Committee's focus on cybercrime. Disgruntled employees and other malicious insiders, competitors, nation-states, hacktivists, and transnational criminal organizations, however, are other common avenues for trade secret theft. Companies need different tools and strategies to protect against each type of threat actor.

Businesses need to be particularly cognizant of risks that arise in their supply chains. The growth in recent years of extended global supply chains, comprising hundreds or even thousands of suppliers, has brought tremendous benefits and given many firms an enormous competitive edge. But companies using extended supply chains often must share confidential and highly valuable business information with their suppliers—many of which may be located in a different country with different laws and different corporate norms.

In the face of this reality, it is absolutely essential that companies implement effective strategies to protect trade secrets not just within their own four walls, but with their suppliers as well. In the CREATe-PwC report, we recommend a five-step approach for safeguarding trade secrets and mitigating potential threats:

- First, companies should identify and categorize their trade secrets throughout their organization.

- Second, they should conduct a risk assessment that identifies both the primary threat actors and potential vulnerabilities in the company's policies, procedures, and controls.

- Third, they should identify those trade secrets that have the greatest impact on the company's operations and business.

- Fourth, they should seek to assess the economic impact that would result from the theft of the most valuable trade secrets identified in step three.

- Fifth, companies should use the data collected in the first four steps to make informed decisions about how to allocate available resources and strengthen existing processes to most effectively increase the company's overall safety profile against trade secret theft.

CREATe recently completed a pilot program with more than 60 companies in countries around the world. We helped these companies assess their vulnerabilities to corruption and IP theft—including trade secret theft—and to implement procedures to mitigate these threats.

Based on that pilot program, we just launched "CREATe Leading Practices," a service designed to help companies improve and mature their management systems. On our website, companies can also find best practices and model policies. Employing these tools proactively can help companies protect their IP assets and remain competitive.

Unfortunately, no amount of protection can completely safeguard all trade secrets from theft. Companies also need a legal system that provides predictable enforcement and meaningful remedies against bad actors. A patchwork of different standards and enforcement mechanisms—whether domestically and internationally—makes protecting trade secrets significantly more difficult.

Recent high-profile criminal enforcement actions are encouraging, and a hearing like this, that highlights the value of trade secrets to the economy, will help prioritize criminal enforcement. Not all instances of trade secret theft are criminal, however, and law enforcement does not have the resources to investigate and prosecute all instances in any event. I am therefore encouraged by the efforts of Senators Coons and Hatch to create a harmonized system for owners of trade secrets to protect their property through a federal private remedy. Senator Flake's interest in theft that occurs overseas is also worth further study and discussion.

Our economy relies on the ability of companies to protect their trade secrets. Governments and companies both play a role in improving protection. In our view, companies would benefit from taking a more proactive role in assessing vulnerabilities and employing best practices to manage their risks. They also need an effective legal system through which to enforce their rights when their know-how has been misappropriated.

Thank you for holding this hearing and for giving me an opportunity to testify. I look forward to answering your questions.

# # # # #

Economic Impact of Trade Secret Theft:

A framework for companies to safeguard trade secrets and mitigate potential threats

February 2014

CREATE.org
Center for Responsible Enterprise And Trade

pwc

About this report

The Center for Responsible Enterprise And Trade (CREATe.org) has collaborated with PricewaterhouseCoopers LLP (PwC) to assess the economic impact of trade secret theft. Our effort has culminated in a report that focuses on four issues that are critical to understanding trade secret theft and how to improve companies' ability to protect their most valuable information:

- an estimate of trade secret theft across advanced industrial economies;
- a threat assessment focusing on what threat actors are most active in targeting trade secrets;
- an original framework for companies to assess the value of their own trade secrets; and
- a look forward 10-15 years in the future to consider what forces and drivers may make trade secrets more or less secure.

Governments, companies and individuals all play a role in improving trade secret protection. It is in every company's self-interest to improve trade secret protection and to use their leverage to encourage the companies they work with to do the same. Creating a shared sense of urgency can enable companies to dedicate resources to improve trade secret protection. Historically, such improvements have been viewed as a cost, not an investment. Our expectation is that this report will help companies shift that calculation of cost versus investment, enable companies to have a better understanding of who threatens their trade secrets and to provide new thinking and tools to help companies secure their trade secrets now and in the future.

Pamela Passman
President and CEO - CREATe.org
ppassman@create.org

Sanjay Subramanian
PwC | Principal
sanjay.subramanian@us.pwc.com

George Prokop
PwC | Managing Director
george.w.prokop@us.pwc.com

Table of contents

Introduction	2
Scope, Approach and Limitations	5
Estimate of Trade Secret Theft	7
Analysis of Threat Actors Engaged in Trade Secret Theft	10
A Framework for Individual Companies to Safeguard Trade Secrets and Mitigate Potential Threats	13
How Do Future Expectations of Trade Secret Loss Impact Private Sector Decisions Today?	24
Conclusion	31
Acknowledgments	32
Endnotes	32

Introduction

In the private sector, trade secrets are fundamental building blocks that drive investment, innovation, and economic growth. The development of trade secrets also benefits the public good by enhancing economic security and stability.

For several years, the theft of trade secrets, often through cyber-enabled means, has been an important issue for the United States and other industrial economies. The deleterious impact of trade secret theft in both the private and public sectors all but ensures that this issue will remain a leading international priority requiring joint solutions to mitigate the ongoing threat and foster greater economic security throughout the international community.

The public sector has expressed a clear willingness to drive policy developments, foster international dialogue across governments, create public-private partnerships and prosecute actors responsible for trade secret theft. The private sector has an equally critical role to play in protecting trade secrets. The private sector's entrepreneurial spirit coupled with investor expectations will continue to drive companies to invest in research and development ("R&D") and develop new and innovative technologies. At the same time, companies must also invest in new measures to identify and mitigate their exposure to trade secret theft by fully understanding their own vulnerabilities and the threat actors targeting their enterprise.

Protecting trade secrets is critical for the continued prosperity and economic security of businesses around the world. In recent years, private and public sector organizations—universities, industry associations, think tanks, and government agencies—have studied this issue in depth. This paper addresses the broader economic issues referenced in other studies (e.g., national level estimates of trade secret theft); however, it primarily focuses on a framework for individual companies to:

1. Apply a risk-based approach to identify and prioritize their trade secret assets;
2. Analyze the direct and indirect economic losses attributable to a trade secret theft;
3. Understand the types of threat actors and how they may seek to inflict economic harm, as well as how those actors align with the company's vulnerabilities;
4. Develop new strategies to safeguard investment underpinning future trade secrets and mitigate the potential economic losses attributable to trade secret theft; and
5. Develop return on investment guidelines for implementing measures to improve trade secret protection internally and in the supply chain.

"The effects of [IP] theft are twofold. The first is the tremendous loss of revenue and reward for those who made the inventions or who have purchased licenses to provide goods and services based on them, as well as of the jobs associated with those losses. American companies of all sizes are victimized. The second and even more pernicious effect is that illegal theft of intellectual property is undermining both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries that can further expand the world economy and continue to raise the prosperity and quality of life for everyone. Unless current trends are reversed, there is a risk of stifling innovation, with adverse consequences for both developed and still developing countries."

– The Report of the Commission on the Theft of American Intellectual Property, 2013

The observations surrounding the assessment of the economic impact of trade secret theft and the accompanying company-level framework are grounded in an analysis of authoritative literature, our collective experience analyzing the economic impact of illicit activities, extensive open source research, our understanding of leading corporate governance and compliance protocols, and feedback garnered from workshops with leading private sector organizations. Our observations from these efforts include:

1. **Estimates of trade secret theft range from one to three percent of the Gross Domestic Product ("GDP") of the United States and other advanced industrial economies.**

Although numerous studies have attempted to analyze the losses attributable to trade secret theft, they have had mixed results, primarily due to concerns about the adequacy, completeness and reliability of private sector information. Beyond concerns about data, the analytic approaches of leading studies vary widely, resulting in disparate estimates of losses. Moreover, concerns about the potential adverse impact to a company's reputation in the market and ongoing relationships with customers limit the type of information companies are willing to disclose – either to industry partners or governments – about trade secret theft or internal vulnerabilities. Notwithstanding the challenges of developing national level estimates of trade secret theft, our analysis leverages multiple studies on illicit economic activity across the United States and advanced industrial nations as a proxy for the theft of trade secrets, resulting in an estimate of 1 to 3 percent of U.S. GDP.

2. **The national level estimate of trade secret theft is important as a guide to policy creation, industry awareness and advocacy, but is less relevant to individual companies.**

At the company level, firms can gain tangible benefits from understanding the relative value of their trade secrets. Analyzing the portfolio of trade secrets that a company keeps and understanding the potential direct and indirect costs (e.g., lost revenue, disruption of business, tarnished reputation) that their theft would inflict is a critical step in a broader company process of prioritizing limited resources to protect trade secrets. In doing so, a company can develop viable estimates on the return on investment it would get from improving trade secret protection, as the probability and severity of a potential breach can be factored into these calculations.

"A consensus among economists has emerged that trade secrets play an important role in protecting the returns to innovation and that trade secret protection is an integral and important part of the overall system of protection available to EU firms to protect their intangible assets, like patents and copyrights."

– European Commission Study on Trade Secrets and Confidential Business Information in the Internal Market, April 2013

---

3. **A company-level approach to estimating losses attributable to trade secret theft will drive more reliable national level results, but companies can do more than serve as the subjects of anecdotes.**

In many instances, companies are referenced in anecdotes about trade secret theft, but refrain from proactive contributions to a broader public dialogue on this issue due to aforementioned concerns about adverse press, stakeholder relationships, market considerations, and/or regulatory exposure. Reticence may also exist because most companies do not yet have standard procedures to consistently or systematically identify or prioritize their trade secret portfolio, let alone consistent means to assess the economic impact of the loss of trade secrets. Better informed dialogue among the private sector, coupled with a framework for considering these complex issues at the company level, may yield substantial long-term benefits to both public and private sector stakeholders.

4. **Increasing company-level awareness of the internal and external threat environment facilitates enhanced protection of trade secrets, an improvement in the quality of the national level estimate of trade secret theft over time, and the potential for a long-term reduction in losses.**

Threat actors come in many forms. Malicious insiders, competitors, nation states, hacktivists and transnational organized crime are only a few examples. Gaining an understanding about who those actors are, their motivations and typologies, and their target selection process can enhance the private sector's understanding of how these actors may seek to exploit a company's vulnerabilities. Similarly, understanding the means by which they go about stealing trade secrets can highlight internal vulnerabilities that companies can prioritize for fixing. For example, while the current focus may be on cyber-enabled means of stealing trade secrets, many threat actors still rely on physical means such as recruitment of insiders and placement of agents within companies for purposes of stealing critical data. Keeping current on trends related to threat actors and their methods helps companies take meaningful steps to better safeguard their assets and mitigate such threats.

5. **Modeling future scenarios highlights the drivers influencing trends in trade secret theft and provides insights that enable companies to create long-term strategies to protect trade secrets.**

By looking forward and considering how threats against trade secrets and other forms of intellectual property may evolve over the next 10-15 years, companies can increase their awareness of how these drivers and factors, if not properly aligned, could make it harder to protect trade secrets. These scenarios can enable companies to visualize and plan for a more secure future for their trade secrets and, at the same time, enhance their ability to make investment decisions today.

6. **Management will be better able to formulate and implement new strategies to safeguard investments and mitigate threat if armed with a greater understanding of current and future trends, threat actors seeking to engage in illicit activity, companies' own trade secret portfolios and organizational vulnerabilities.**

To maintain competitive advantage in the global marketplace, companies will continue to make significant investments to develop new products and services, the protection of which will be critical. Coupled with the consistent threat of a trade secret theft event and the deleterious impact it can have, management can justify the need to increase company, supply chain and business partner awareness of the threats and trends, and implement protective measures to safeguard these valuable investments. These protective measures can include improved IP protection management systems and improved technology.

Scope, Approach and Limitations

CREATe.org and PwC collaborated to (i) analyze the economic impact of trade secret theft in advanced industrial economies, and (ii) develop a company-level framework to aid the private sector in its efforts to address this important issue. This study furthers CREATe.org's mission as a non-profit organization dedicated to helping companies and their suppliers and business partners reduce counterfeiting, piracy, trade secret theft and corruption.

Definition: Trade Secret

For the purposes of this report, we use the definition of a "trade secret" set forth in the U.S. Economic Espionage Act ("EEA"). It is similar to the definition of trade secrets under the Uniform Trade Secrets Act that has been enacted by 47 U.S. states and several U.S. territories, consistent with Article 39 of the World Trade Organization's Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) and Article 2 of the Japanese Unfair Competition Prevention Act. Under the EEA, trade secrets are:

...all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, analyses, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if - (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public...[2]

Approach

This study is based in part on CREATe.org's efforts in the market to heighten trade secret awareness, increase and improve collaboration amongst companies and between the private and public sectors, and assist companies in fostering a better understanding of the tools companies have at their disposal to categorize, document, and protect their trade secrets through improved management systems and utilization of technology.

Our approach reflects the significant and growing body of literature on the topic of trade secret theft. It estimates the losses attributable to trade secret theft across advanced industrial economies using a proxy approach that measures other forms of illicit economic activity. However, recognizing that this approach only serves as an estimate, we collectively developed a framework to assess the economic impact of a trade secret theft event at a company level by applying more traditional economic analyses and techniques. The framework relies on dual methodologies including: (a) a direct method to estimate the lost future revenue and profitability associated with the theft of a trade secret, and (b) an indirect method evaluating the more intangible adverse impacts of such an event, as measured through various non-financial performance indicators. Our approach incorporates inputs on threat actors, probability and severity of incidents, organizational protections and vulnerabilities, and future trends analysis that companies should consider. These inputs drive the economic impact of a trade secret theft event and are important elements that companies should factor into their assessment of how to protect their trade secrets. In this context, the study may be viewed as a guide for individual companies, and as a path forward to a future national level estimate.

The study is broken into the following phases:

1. An estimate of trade secret theft across advanced industrial economies;
2. An analysis of the threat actors who are actively engaged in trade secret theft;
3. A framework enabling companies to conduct their own internal evaluations and inventories of existing trade secrets, assess their vulnerabilities to loss, estimate the economic impact of a trade secret theft event, and provide new insights on how to protect these assets; and
4. An outlook for the future of trade secret theft using the results of a futures modeling exercise—drawing from workshops with private sector participants—that present scenarios for future developments and concerns.

Taken together, these sections represent a broad approach to evaluating the aggregate impact of trade secret theft by starting at the company level, and giving companies the tools needed to effectively manage and protect their trade secrets. This practical approach recognizes that fostering greater activity and awareness of this issue among individual companies may produce significant advancements on this challenge.

Our approach reflects the significant and growing body of literature on the topic of trade secret theft.

Limitations

The framework is an approach we collectively developed based on our experience and interaction with numerous companies and organizations facing trade secret theft. It is meant to serve as a guide for companies to document and analyze their trade secrets so they may apply their resources in a cost effective and efficient manner. Application of the framework will not necessarily prevent a trade secret theft event, but may enable companies to better identify and mitigate threats as they arise due to greater understanding of the threat landscape and their internal vulnerabilities, and to be more strategic in allocating resources to protect their trade secrets.

Our outlook section in which we discuss the results of our futures modeling exercise addresses how trade secret theft issues may play out globally, not only in the U.S. The scenarios should not be read as predictions, but rather as a survey of how trends could evolve under certain future conditions. They were created using four drivers in different combinations. These drivers are only four among many that will likely play a critical role in trade secret protection in the years ahead.

Estimate of Trade Secret Theft

Estimating the value of trade secrets at a national or global level presents significant challenges. In this section we will address these challenges and present an approach to estimating the economic impact of trade secret theft.

Obstacles to Estimating Trade Secret Value

Trade secrets, intellectual property ("IP"), and other intangible assets represent a large and growing share of U.S. and global economic activity. The growing number of patents issued by the U.S. Patent and Trademark Office illustrates the essential role intangible assets play in supporting a dynamic global economy. From 1990 to 2010, the pace of innovation in the private sector spurred the growth of intellectual property and the number of patents issued in the U.S. increased by 40.6 percent, jumping from 99,200 patents issued in 1990 to 244,300 in 2010. Notwithstanding the central and powerful role that IP plays in the global economy, there is no consensus on the exact value of trade secrets or how to estimate such a figure.

Numerous academic, industry, non-profit and government reports highlight the challenges in estimating the overall value of trade secrets and the economic impact of those that are stolen. For example, a May 2013 study by the Commission on the Theft of American Intellectual Property ("Commission")—an independent and bipartisan group chaired by Admiral Dennis Blair and Ambassador Jon Huntsman—assessed various dimensions of international IP theft and its impact on American businesses. The Commission concluded that the exact value of IP theft was "unknowable," but added that existing assessments of loss have underestimated the impact of IP and trade secret theft. The Commission offered three explanations for why trade secret value was so difficult to measure:

1. Loss is measured in different ways in different sectors;
2. Companies do not often report their losses and are not incentivized to do so out of fear of impact on stock prices and marketplace reputation; and
3. Surveys are often used to measure loss and they are not sufficiently dependable to offer details on such a vast problem. [5]

In another example, a 2010 Government Accountability Office ("GAO") study analyzed the economic effects of counterfeit and pirated goods and found that "it was not feasible to develop our own estimates [of the total value of counterfeit or pirated goods] or attempt to quantify the economic impact of counterfeiting and piracy on the U.S. economy."[6] Noting the lack of data as a primary challenge to quantifying the economic impacts of counterfeiting intellectual property and goods, the GAO concluded that "neither governments nor industry were able to provide solid assessments of their respective situations" suggesting the need for individual companies to evaluate the worth of their own trade secrets.[7]

After reviewing these and other studies, as well as conducting an independent analysis of trade secret theft, we noted additional considerations that impede estimation of the value of trade secrets:

- The volume of data required to construct an accurate assessment that withstands scrutiny is significant, and would face substantial legal and analytic challenges;
- Some companies are simply unaware that their trade secrets have been stolen, while other companies are reluctant to report such losses to third parties due to concerns about reputational or financial repercussions; and
- Such an assessment would by its nature be somewhat fleeting. As soon as such a figure was agreed to, the value of the trade secrets at the heart of the analysis would have already begun to shift across individual companies or industry sectors.

Purpose of Utilizing Proxies to Estimate Trade Secret Theft

Given the inherent methodological challenges of estimating the value of trade secrets at a national or global level, a proxy approach to estimating the value

of trade secrets can be useful and provides interesting insights. Seemingly unrelated activities—such as research and development spending, occupational fraud, and tax evasion—share important traits with trade secrets, and provide insightful context that enables reasonable estimation of the economic impact of trade secret theft.

Proxy for the Value of Trade Secret Theft: Research and Development

A core proxy for the value of trade secrets involves private sector expenditures on R&D. There are numerous valuable trade secrets that are not related to R&D (such as customer lists, sales data, marketing information, etc.) but R&D represents investment in new ideas, methods, tools and techniques—each of which are critical elements of many trade secrets. Since the early 1980s, R&D expenditures in the United States have exceeded 2.5 percent of GDP; U.S. Government figures report the figure as $414 billion or 2.7 percent of GDP in 2011.[8]

Global R&D investment trends are similar to U.S. trends. Battelle and *Research & Development Magazine's* 2014 "Global R&D Funding Forecast" examine global R&D for the top 40 world economies (ranked by nominal GDP) and levels of actual and projected spending. As illustrated in Figure 1, they conclude that R&D for the top 40 national GDPs averaged nearly 2 percent in the last three years and are forecast to maintain this level in 2014. Over the last three years, R&D as a percentage of global GDP has also remained steady at 1.8 percent.[9]

Current R&D spending, of course, generates other forms of trade secrets, and represents only a fraction of the economic value generated by R&D. Researchers have estimated that $1.00 of spending on R&D produces about $2.90 in other economic activity during the same year and between $16.00 and $69.00 over the next 10 years.[10,11] On this basis, the value of trade secrets in the marketplace represents a significantly greater component of GDP than illustrated by R&D spending alone.

Proxy for the Estimate of Trade Secret Theft: Illicit Economic Activity

Proxies involving illicit economic activity also clarify the potential impact of trade secrets theft. Such measures capture economic behavior that may inflict harm on the global economy and, like trade secret theft, are under-

Figure 1: R&D as a percentage of GDP

	2011	2012	2013	2014
U.S.	2.7%	2.8%	2.8%	2.8%
China	1.5%	1.8%	1.9%	2.0%
Japan	3.5%	3.4%	3.4%	3.4%
South Africa	1.0%	1.0%	1.0%	1.0%
Germany	2.9%	2.8%	2.8%	2.9%
Australia	2.3%	2.3%	2.3%	2.3%
UK	1.8%	1.8%	1.8%	1.8%
Russia	1.5%	1.5%	1.5%	1.5%
Qatar	2.8%	2.8%	2.8%	2.7%
Brazil	1.2%	1.3%	1.3%	1.3%
Average (Top 40)**	2.0%	2.0%	2.0%	2.0%
Rest of World	0.4%	0.4%	0.4%	0.4%
Global Average	1.8%	1.8%	1.8%	1.8%

*2014 figures are projected

**Top 40 world economies by GDP

Sources: 2013 & 2014 Global R&D Funding Forecase, Battelle and R&D Magazine.
Sub-Sources: IMF, World Bank, CIA World Fact Book

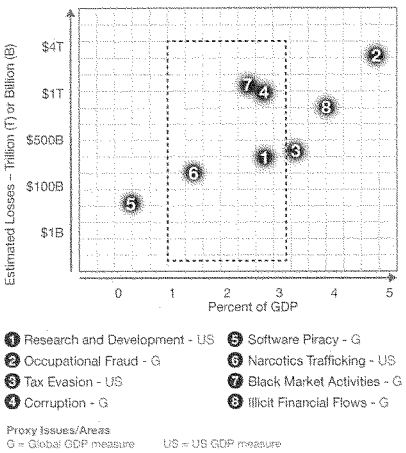
reported and difficult to measure. Also, in a manner similar to their approach to trade secrets, certain threat actors will target these areas for a variety of economic (e.g., market share, profitability) and non-economic (e.g., increase influence, advance social causes) reasons:

- *Occupational Fraud:* Companies worldwide lose as much as $3.5 trillion, or 5 percent of global GDP, due to occupational fraud and abuse, according to a 2012 report based on the analysis of nearly 1,400 fraud cases by the Association of Certified Fraud Examiners ("ACFE").[12] Facing a similar set of threat actors as trade secret theft—namely malicious insiders with unparalleled access to systems, these perpetrators make measuring fraud and abuse difficult.
- *U.S. Tax Evasion:* In a 2013 study the U.S. Internal Revenue Service ("IRS") estimates the tax gap—the difference between what taxes are owed and what taxes are collected—to be approximately $450 billion, or 3.25 percent of U.S. GDP. The IRS assesses that the tax gap is a result of nonfiling, underreporting and underpayment—and that it can be challenging to determine what activity is illegal.[13]

- *Corruption:* Another significant issue that often defies exact accounting is global corruption, defined traditionally as the abuse of public office for private gain. Like trade secret theft, corruption poses a unique threat to both the public and private sector by eroding confidence in the rule of law as well as undermining competition. A study sponsored by the World Bank estimates the annual cost of such activities as some $1 trillion, or 2.9 percent of global GDP in 2005.[14]
- *Copyright Infringement and Software Piracy:* Copyright theft, copyright infringement and software piracy are widely recognized challenges for advanced industrial economies. A 2012 Business Software Alliance ("BSA") report noted, for example, that some 42 percent of global personal computer users employ pirated software, reaching a commercial value of $64.3 billion in 2011, or 0.1 percent of global GDP. A diverse group of threat actors targeting trade secrets may also be interested in pirating software. Criminal groups are known to pirate software strictly for profit, while hacktivists may attempt to damage the reputation of software companies by creating pirated software that damages systems and users, resulting in negative publicity for the software's true originators.[15]
- *Narcotics Trafficking:* Like the theft of trade secrets, the trafficking of narcotics inflicts a variety of economic costs, including workers' lost productivity, medical treatment, and the administration of justice. In a 2011 study of the impact of illicit drug use in the United States, the U.S. Department of Justice estimated the cost in 2007 to be as high as $193 billion, or about 1.4 percent of U.S. GDP in 2007.[16]
- *Black Market Activities:* At the global level, the value of black-market activities is estimated at $1.8 trillion—approximately 2.5 percent of global GDP—according to information compiled on the crowd-sourced database Havocscope. This estimate includes a diverse range of activities that are challenging to quantify: counterfeiting of products like aircraft parts, food, weapons, cosmetics, watches, and clothing; trade in endangered wildlife; art theft; illegal gambling; bootlegging of tobacco and alcohol; and human trafficking.[17]
- *Illicit Financial Flows:* The illegal movement of money from developing countries to financial institutions in developed states is, in some ways, a mirror image of the theft of trade secrets, which typically involves the illicit transfer of sensitive information in the opposite direction. In a 2013 study of 55 developing countries funded by the Ford Foundation, economists' estimated that illicit financial outflows—most in the form of mis-invoicing of trade—amounted to $947 billion in 2011, some 3.7 percent of these countries' combined GDP.[18]

Taken together, these proxy measures provide context for trade secret theft as yet another form of illicit economic activity and corroborate its significant impact on national economies. As illustrated in Figure 2, most of these measures are clustered between 1 and 3 percent of GDP. While it is difficult to accurately measure economic losses attributable to trade secret theft at a national or industry level, this proxy approach provides a reasonable estimate of the economic impact of trade secret theft given the similarities between trade secret theft and other forms of illicit activity.

Figure 2: Proxies for Estimate of Trade Secret Theft



Analysis of Threat Actors Engaged in Trade Secret Theft

Numerous actors—foreign intelligence services, competitors, transnational criminal organizations, hacktivists and malicious insiders—target and steal companies' trade secrets for various reasons. Social engineering schemes such as tailored spear-phishing campaigns that implant malware to steal trade secrets, or duping employees into revealing sensitive corporate information, exemplify the means by which these actors engage in trade secret theft. Constantly evolving technologies in smart phones, laptops, and tablets that employees use for work provide additional means for threat actors to access a company's secrets. Threat actors' motivations are equally diverse. Some seek personal financial gain, while others hope to advance national interests or political and social causes.

Many threat actors are known to target and steal trade secrets. The threat actors profiled in this section were selected using a risk-based methodology that considered several factors:

- A well-documented track record of attacking multinational companies;
- Intent to misappropriate companies' trade secrets and critical data;
- The capability, as demonstrated by past attacks and by U.S. and other government reporting, to target companies' trade secrets for their own profit or to advance another country's interests;
- Intent to attack companies and institutions that are rich in trade secrets and other valuable corporate data;
- Consistent focus on specific industries and sectors—information and communications technology, aerospace & defense, marine systems, clean technologies, advanced materials and manufacturing, healthcare and pharmaceuticals, agricultural technology, energy and natural resources—consistent with the 2011 Economic Espionage Report;[19] and
- Demonstrated impact on companies due to the theft of trade secrets.

The more effectively that companies can understand these actors and their respective typologies, the better equipped they will be to manage their trade secret portfolios and apply appropriate protection measures that are calibrated to the economic value of specific trade secrets, the type of actor and the type of threat. Companies able to understand who may seek to steal their trade secrets are better able to view those secrets through the lens of a threat actor, and therefore apply appropriate resources to enhance their security.

Nation States

Nation states have unmatched resources and capabilities for stealing trade secrets, and usually want to acquire foreign trade secrets to strengthen their existing military capabilities and bolster national champion companies in the global marketplace.[20] Many foreign intelligence and security services attempt to acquire trade secrets and sensitive economic information on behalf of their governments, commonly using covert means. Nation states may also use other national agencies, regulatory powers, or state-supported organizations. Some even publicly claim this is part of their missions. For example, the decree establishing Russia's Foreign Intelligence Service assigns it responsibility for "protecting the country's economic development and scientific progress."[21] Other examples of nation state actors trying to collect trade secrets from companies include:

- The head of a German satellite company told U.S. diplomats in 2009 that France represented a greater danger to his country's IP than any other country.[22]
- In 2011, a former employee of a major American chemical company pled guilty to committing economic espionage that benefitted elements of the Chinese government.[23]
- South Korean intelligence officers have been found trying to obtain economic secrets from Australian officials in 2013, according to multiple reports.[24]

Malicious Insiders

Current and former employees, third parties acting as consultants or lawyers, and suppliers often have unique access to corporate trade secrets and other information that, if released, could inflict significant harm on a company. Respondents to PwC's *2013 U.S. State of Cybercrime Survey* identified current and former employees as one of the greatest cyber security threats they faced.[25] Insiders' knowledge of companies' systems, where and how information is stored, and specific details on the production or use of trade secrets makes insiders a uniquely dangerous threat. The threat from malicious insiders is all the greater because insiders often cooperate with other threat actors who can provide money, other resources, or ideological motivation. Examples of the cost insiders inflict on companies with high value trade secrets include:

- In 2012, a former employee of a North American automotive company and the employee's spouse were found guilty of stealing trade secrets related to hybrid vehicle technology worth $40 million. The couple intended to sell the information to a Chinese competitor.[26]
- An employee of a large U.S. futures exchange company pleaded guilty in late 2012 to stealing more than 10,000 files containing source code for a proprietary electronic trading platform. Prosecutors estimated the value of these trade secrets between $50 and $100 million. The employee said he and two business partners had planned to use this source code to develop their own company.[27]
- In 2011, a former employee of an automotive company was sentenced to 70 months in prison for copying some 4,000 documents on the design of engine-transmission and electric power supply systems. The employee intended to take these documents to a new job with the China branch of another North American company.[28]

"Ultimately, cybercrime is not strictly speaking a technology problem. It is a strategy problem, a human problem and a process problem."

– PwC Global Economic Crime Survey, 2014

Cultural and technological factors may heighten the insider threat in coming years. A study noted that the nature of U.S. employees' loyalty to their employers is changing because of the much higher rate of lifetime job changes in the 21st century, as compared to the mid-20th century. At the same time, growing numbers of people with highly sought-after technical skills often cross international borders for work, which means more employees with potentially competing sources of loyalty. Additionally, the growing prevalence of "bring your own device" policies and the ease and speed with which employees can move data across multiple programs and applications hampers security and monitoring efforts. These factors could increase the population of malicious insiders with increased access and a diminished sense of obligation to their employer – factors that may increase the risk that they will use their status to expose trade secrets and other sensitive corporate data.[29]

Competitors

Competitors can target companies' trade secrets independently or with assistance from national governments; cases involving competitors stealing trade secrets represent a large portion of U.S. Department of Justice trade secret theft cases. From these cases we see that competitors can use several methods, including recruiting employees of the targeted company who are disgruntled or have personal ties to the competitor's home country to steal trade secrets or sensitive corporate data. Other methods include bribery, extortion, or the promise of a new job.

Even when acting independently of national governments, corporate competitors often have the resources to exercise state-like power. The repeated use of insiders and corporate spies to access critical and sensitive data is illustrated by recent trade secret theft cases involving competitors:

- A sting set up by U.S. law enforcement uncovered attempts to bribe an undercover agent posing as a corrupt lab technician of a major U.S. pharmaceutical company that had recently spent millions to develop formulas for a new drug. The indictment noted that the successful theft of the formula could have resulted in billions of dollars of losses for the company.[30]
- In a case involving Asian and North American chemicals companies, the Asian firm is alleged to have hired current and former employees of the North American company as consultants in order to have them reveal confidential and proprietary information. This enabled the Asian company to replicate a proprietary manufacturing process and earn at least $225 million in proceeds from the theft of the trade secrets.[31]

Transnational Organized Crime ("TOC")

Transnational Organized Crime groups have successfully attacked numerous corporate information technology networks to access payment systems and steal personally identifiable information, personal health information, and payment card information, inflicting massive financial damage on their targets.[32] As TOC groups expand their activities beyond long-standing activities such as gambling or racketeering, many well-established groups are increasingly leveraging the Internet for all manner of cybercrimes.[33] In this role they are serving as facilitators that enable other threat actors, such as unscrupulous competitors or intelligence services, as they attempt to steal trade secrets.[34]

A computer security company recently noted the emergence of "cybercrime-as-a-service,"[35] and TOC groups often work with other established cyber criminals, purchasing information they have stolen via electronic means for the purposes of furthering their own traditional organized crime agendas.[36] In 2013, the Director of National Intelligence warned that cybercriminals could "enable access to critical infrastructure systems or get into the hands of state and non-state actors." This dimension of cybercrime is increasing the availability of hacking tools that can be used to steal trade secrets, potentially allowing threat actors to easily rent or buy sensitive corporate or other information.[37]

Hacktivists

Hacktivists seek to expose sensitive corporate information—potentially including trade secrets—to advance political or social ends. These groups have used cyber intrusion skills and data gleaned from disgruntled insiders to obtain and publish Personally Identifiable Information (PII) and sensitive business information of key executives, employees, and business partners. As with TOC groups, hacktivists have the technical knowledge and capabilities to steal trade secrets, and they could partner with other threat actors for ideological or financial reasons.

Greater awareness of the threat actors attempting to steal trade secrets, their capabilities, and typologies can position company management to understand their vulnerabilities to theft by these actors and to formulate and implement strategies to mitigate these threats. The following section incorporates this understanding and lays out a scalable framework that companies can use to (i) assess the company-level economic impact attributable to trade secrets theft, and (ii) enhance their ability to safeguard investments and mitigate future losses.

A Framework for Individual Companies to Safeguard Trade Secrets and Mitigate Potential Threats

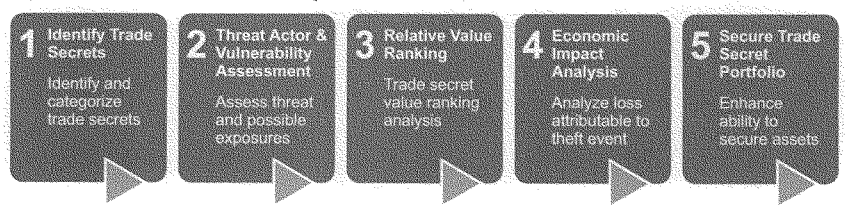
The growing threat of trade secret theft and the adverse economic implications it creates for the private sector require companies to be increasingly proactive in managing this threat to achieve their strategic, operational and financial goals.

In response, CREATe.org and PwC developed a multi-level framework for private sector organizations to analyze their trade secret portfolios. The framework provides a platform to identify and categorize trade secrets leading to an analysis that yields insights into threat actors seeking to induce economic harm, vulnerabilities in companies' existing control structure and a model to assess losses attributable to the theft of a trade secret. Collectively, this framework provides companies with a means to identify potential gaps or exposures in their trade secret protection strategies and ideas to further their ability to safeguard their investment and mitigate future losses. It also provides critical information that enables companies to better understand the return on investment of improved trade secret protection and how to strategically allocate resources. An illustration of the framework is presented in Figure 3.

This section of the paper describes the activities and key points for management's consideration for each level of the framework. As a reference to illustrate the framework's application, each level provides further explanatory guidance on how *ABC Widgets, Inc. ("ABC")* proceeds through the framework. *In our example, ABC is a large, global, publicly-traded, U.S.-based alternative energy company, with a widely-dispersed third-party supply chain and aggressive plans to expand into new markets.*

In our scenario, ABC's executives and board members are becoming increasingly aware of advanced threats to its intellectual property and, in particular, its trade secrets based on recent media reports about attacks against ABC's competitors. At a quarterly board meeting, ABC's directors question management about its plans to mitigate such threats. Reluctantly, ABC's management acknowledges that they have not yet thoroughly identified its portfolio of trade secrets, nor implemented a trade secret protection management system, and will quickly endeavor to analyze these issues with the goal to seek opportunities to strengthen the company's ability to mitigate such threats.

Figure 3: A framework for assessing the business impact of trade secret loss



Level 1: Identify Trade Secrets

Our collective experiences indicate that many companies fail to effectively manage their trade secret portfolios for multiple reasons, including a lack of consensus on what assets actually constitute the portfolio. Some companies' reticence may also stem from their interpretation of "reasonable measures [are] taken to protect [trade secrets] the information"[38]—mistakenly deducing that any specific documentation of trade secrets potentially creates exposure for the company in the event of a breach. Reasons for this could include concerns about incomplete documentation, lack of follow through, or other such errors or inconsistent practices, but the net result is the fear that courts will find the company has not met the reasonable measures standard. Such companies may prefer taking a general, blanket approach to security and confidentiality that could apply to any information the company may later identify as a trade secret. Our view is that individual companies must weigh the benefits of this thorough approach against the risks, costs, and the company's ability to abide by the basic tenets of the framework, while also considering the risks inherent in not closely protecting the company's most sensitive trade secrets.

This first level of the framework takes the organization through the basic, yet critical step of identifying and categorizing its trade secrets. To best protect those trade secrets whose theft would cause the most harm, companies should first document, locate and inventory their trade secrets. This first step gathers key stakeholders—senior executives, business unit leaders, corporate functional leaders—to inventory the trade secrets maintained by the company. Ultimately, forming a cross-functional team with senior management support is critical to this step and those that follow. Discussion and debate of what constitutes a trade secret for the company is encouraged, as stakeholders should emerge from Level 1 with a broad consensus of not only the definition of a trade secret for their company, but also a list of the company's trade secrets aggregated into categories such as those summarized in Figure 4.

In response to the Board of Directors' queries, ABC embarks on a process to identify its trade secrets. ABC's Compliance Counsel is designated by ABC's Executive Leadership Team to lead the effort. Having recently attended a conference on intellectual property matters, she too started to become aware of the emerging threats to ABC's trade secrets.

Figure 4: Trade Secret Categories

Category of Trade Secrets	Examples
Product Information	New hardware designs; adaptations/updates of existing products
Research & Development	Long-term R&D; basic or applied research; geology R&D
Critical & Unique Business Processes	Inventory/distribution; manufacturing processes; business model based on application of processes
Sensitive Business Information	M&A prospects/plans; market research/studies; customer list/information; information on key suppliers/business partners; expansion plans; corporate strategy
IT Systems and Applications	Novel application of IT that could create new markets; system architecture designs; source code; algorithms

She researches applicable laws, regulations and standards governing trade secrets. She also studies ABC's existing policies and determines that ABC does not maintain a central repository or conduct standardized procedures to manage their portfolio of trade secrets. Recognizing that much work needs to be done, she initiates a working session with a cross-functional team of ABC's senior executives, business unit leaders and corporate functional leaders to inventory the company's existing trade secrets across the categories highlighted in Figure 4.

Before the working session, ABC's Compliance Counsel distributes a working definition of a trade secret and encourages participants to engage in a lively debate. Participants arrive at the working session with their lists, which they present, discuss, and compile into a master list that aligns with ABC's views about what constitutes a trade secret. The meeting results in a categorized list of valuable trade secrets reflecting critical elements of ABC's business model.

Following the working session, the Chief Information Security Officer ("CISO") tasks staff to leverage technology solutions to search across the organization for the assets identified during the working session. Using tools that search based on keywords and other identifiers, trade secrets from the master list are found on various servers, in files with non-relevant file names, and on shared-file sites created for reasons unrelated to the trade secret itself. The results for the location of each trade secret found are noted on the master list, to be incorporated later into the vulnerability assessment. The CISO will also work with other business leaders to find trade secrets—which could may exist off the network, in hand-written notes, prototypes, etc.—to ensure that as many trade secrets as possible are located regardless of their presence on IT systems.

By completing Level 1, companies have an agreed-upon list of a company's critical trade secrets—a critical first step in this framework. Many of the trade secrets are also located across the organization, which will contribute to understanding how vulnerable they are to theft. However, as organizations continue to design new technologies or engage in new ventures, they will continue to develop and/or acquire new trade secrets. Therefore, management must establish procedures to continuously refresh this inventory on a periodic basis to facilitate its completeness.

Level 2: Threat Actor and Vulnerability Assessment

A risk assessment focused on threats and vulnerabilities forms a critical step in the framework. As noted earlier, threat actors take many different forms, each of which poses a significant threat to a company's intellectual property. Analysis of existing trade secret protection management systems—the compliance and security program policies, procedures and internal controls—enable management to identify vulnerabilities in its current protocols that may create unnecessary risk and exposure for the company. Evaluating the maturity of the overall trade secret protection program and the specific processes is an effective way to understand the vulnerabilities.

2.1: Threat Actor Assessment

Operating in today's global marketplace exposes companies to unique and varied threat actors. As such, management must understand the scope of the company's operating environment (e.g., office locations, sales/marketplace footprint, supply chain, product/service mix, key personnel, and growth strategies) in context of the potential threat actors seeking to engage in illicit activity to adversely impact the company. Assessing the risk posed by individual threat actors within this construct, the probability that they will attempt to steal a company's trade secrets, and the severity of such an event, is critical to determining which trade secrets merit the highest level of protection and enables management to implement more effective protective measures.

As part of its threat assessment, ABC's Compliance Counsel analyzes the company's operating environment, including markets in which the company operates, major customers, significant supply chain and business partners, key executives, employees' access to trade secrets, existing products/services, and designs for new product launches and/or mergers and acquisitions (M&A) activity.

In this context, ABC analyzes the various threat actors that may impact its operating environment and the risk they pose, paying particular attention to the probability and potential severity of a breach. With ABC's leading market position in the industry, it suspects certain threat actors (i.e., malicious insiders, nation states) warrant closer attention and monitoring due to recent data breaches resulting in the theft of intellectual property at ABC's competitors in locations where ABC also has production facilities. Using Figure 5 as a general guide, ABC researches recent incidents to understand the potential threat actors targeting the company and the likelihood of a malicious action from them.

Figure 5: Potential Threat Actors' Goals, Tools, Vectors and Targets

Threat actor	Goals	Tools and vectors	Trade secrets that could be targeted in your firm
Nation states	• Technology to support military capabilities • Strengthen "national champion" companies	• Foreign intelligence and security services • Cyber vector • Human intelligence operations • Technical tools such as electronic eavesdropping, acoustic cryptanalysis, video surveillance and wiretaps • Use of insiders • Exploitation of open source information concerning companies' executives, vulnerabilities or projects. • Co-opted entities such as state-owned enterprises	• Items with direct military applications, such as aerospace technologies • "Dual-use" products, such as IT technologies and navigational systems, with both civilian and military applications
Malicious Insiders	• Competitive advantage • Financial gain • Advance national goals	• Access to sensitive company information • Manipulation of weak protections, lack of oversight over trade secrets • Can access trade secrets on electronic/IT systems or that are hardcopy only	• Data that enables your firm to differentiate its services and products in your sector, such as source code or marketing plans • "Dual-use" products • Sensitive data on customers or suppliers
Competitors	• Competitive advantage	• Cyber vector • Technical tools such as electronic eavesdropping, acoustic cryptanalysis, video surveillance and wiretaps • Use of insiders • Exploitation of open source information concerning companies' executives, vulnerabilities or projects.	• Data that enables your firm to differentiate its services and products in your sector, such as source code or marketing plans
Transnational Organized Crime	Financial gain • PII, other financial data • Cybercrime as a service sold to others	• Cyber vector • Some TOC groups willing to undertake physical attacks against company leadership, personnel and facilities • Use of insiders • Exploitation of open source information concerning companies' executives, vulnerabilities or projects.	• Any trade secret perceived as vulnerable to exploitation
Hacktivists	• Advance political or social goals by exposing sensitive corporate information	• Cyber vector • Exploitation of open source information concerning companies' executives, vulnerabilities or projects.	• Sensitive data on customers or suppliers • Production/distribution technologies

2.2: Vulnerability and Protection Analysis

Threat actors often seek to exploit vulnerabilities in an organization's governance, financial, technology, operational or compliance architecture leading to opportunities for illicit behavior that create economic harm to the company. Accordingly, companies must proactively identify potential internal vulnerabilities in their policies, procedures and controls, as well as their reliance on suppliers and other business partners, and take steps to mitigate any exposure resulting from these weaknesses. These vulnerabilities can range from a lack of training on information security to employees using software without routinely checking for updates, to a highly valuable trade secret stored on an unsecured server with broad access within the company, to a lack of awareness among employees of where trade secrets are kept. Trade secrets can be gauged on a continuum from "fully protected" to "unprotected," and a narrative documenting the type and strength of protection, as well as the remaining vulnerabilities, can be attached to each trade secret. A critical component of the vulnerability assessment is to assess the maturity of the trade secret protection management system.

For each trade secret identified and located during the Level 1 inventory analysis, ABC's Compliance Counsel collaborates with senior executives and corporate functional leaders (e.g., CFO, CIO, CSO, CISO) to review where the information is stored and catalogs the existing protections. ABC also analyzes and documents the design and operation of the existing suite of policies, procedures and internal controls designed to secure and/or limit access to that trade secret. Through this process, ABC's management becomes aware of potential gaps—vulnerabilities—in its existing compliance/security architecture that may require new investment to strengthen and/or enhance efforts to mitigate the risks associated with the combined threat and vulnerabilities. They also identified processes within their trade secret protection management system that were weak and would require improvement. ABC leverages a traditional risk and control matrix to document its analysis, thereby facilitating a discussion with management; an abbreviated example is included as Figure 6

Figure 6: Threat and Vulnerability Matrix

Trade Secret	Threat Actors	Probability of Trade Secret Theft Event (high, medium, low)	Severity of Trade Secret Theft Event (high, medium, low)	Existing Policies, Procedures, Controls, and Mitigating Actions	Severity of Trade Secret Theft Event (high, medium, low)
Source Code	• Nation state X • Competitor Y • Competitor Z	High	High	• Information Security policy • Limited access to local development group, November 2013 • Source code located on a secure server • Access control list to source code • Document handling standard	Medium • We lack a consistent training program • We have found instances of source code being circulated • We have not conducted attack and penetration testing against our servers in the past year.

Protecting Trade Secrets: At What Cost to Collaboration?

Companies often raise concerns that taking steps to limit access to trade secrets by implementing stringent security measures has the inadvertent effect of creating "work arounds" in which employees create unofficial processes and means to access trade secrets so as to avoid encountering the security measures—for example, mandating a highly complicated password to access sensitive documents leads to employees writing the password on a note and keeping it in their desks where other staff may find it. While this would be a violation of company policy, employees may be doing so in order to "get the job done", collaborate, and operate efficiently.

Companies must select the appropriate level of security controls for their unique corporate culture, the amount of time and resources to be invested in training and awareness campaigns. Once these issues are addressed, create clear policies and processes articulating the responsibilities of individual employees. Compliance monitoring and periodic analysis should also be implemented.

For example, since many of ABC's trade secrets relate to its source code, its vulnerability analysis targets the security of its information technology systems and the access controls surrounding the systems. ABC engages in discussions with its CISO, who identifies the security controls that are currently in place for the identified systems. They debate whether these controls are well understood by company employees, and review policies and training programs that support them. The team discusses the potential vulnerabilities of each level of protection given the known and suspected threat actors who may be targeting the company.

The cross-functional team responsible for the overall trade secret protection management system begins to realize the difference between IT security and trade secret protection. This major realization impacts how they proceed to develop a plan that integrates both. At this stage, ABC acknowledges these vulnerabilities and develops recommendations for enhanced mitigation.

Level 3: Trade Secret Portfolio Relative Value Ranking

With only limited resources to implement new safeguards around its most critical assets, how should management decide which trade secrets deserve greater protections? How should management rank its trade secrets based on the insights garnered from the initial analyses performed in Levels 1 and 2?

A Relative Value Ranking analysis provides the company with the means to conduct a qualitative assessment using value-based judgments on the relative importance of a trade secret so that it can perform an initial selection of trade secrets that have the most significant impact on the operations and performance of the business.

Following completion of Level 1 and Level 2, management has new and critical insights into the scope and extent of their trade secret portfolio, including potential areas of vulnerability and threat actors who may seek to inflict economic harm on the company. Depending on the company, these analyses may have provided insights into dozens of trade secrets that the company maintains; some of which are clearly more valuable or create more exposure than others. This value ranking is a critical in developing a return on investment (ROI) proposition that management can use to justify investing more resources in trade secret protection and IT security.

Figure 7 provides an illustrative series of questions to aid management's ability to prioritize those assets among its trade secret portfolio based on the insights from Levels 1 and 2. A related scoring methodology then yields a ranked version of the portfolio based on management's risk assessment of the assets. In order to safeguard the ranked list, companies may consider putting the process and ranked results under attorney client privilege to prevent a defense team from later claiming in court that lower value trade secrets should translate into lower value damages awards.

Following completion of its Level 1 and Level 2 analysis, ABC's Compliance Counsel gathers ABC's executives to evaluate the questions in Figure 7 and rank each asset. For each trade secret, ABC uses these questions to assess the dimensions of the asset's value to the business. In this instance, the relative weights of "Low",

Figure 7: Establishing the Relative Value Ranking for Company Assets

	High	Medium	Low
How significantly would the company's reputation be impacted if this trade secret were compromised?	We would have devastating reputational impacts	We would likely have some reputational damage that we would have to respond to and manage	Not very, may have some residual effects but we could recover from them
How critical is this trade secret to the fundamental operation of the business?	It is absolutely critical and there are no viable alternatives	It is critical but we could find an alternative if absolutely necessary	It is not critical to our business operations
How core is this trade secret to our corporate culture that its loss or theft would have a strong emotional impact on the corporate culture?	This is at the core of our culture and would have a devastating impact on morale and our identity	This is core to our business and its loss would be felt by our employees but we would recover fairly well	It is not a core component of our corporate culture
Is this trade secret especially unique to the industry or is a similar product being used/sold?	We are the only company in the industry that makes/sells/uses this	Other companies make/sell/use it but our version has an exceptional characteristic that makes it unique	No, many other companies make/sell/use something similar
Could competitors place a higher value on this trade secret than we do?	Yes, this can be used for many more purposes that we use it for and therefor	Maybe, but we are unaware of how it may be valued differently	No, its value is consistent across the market
How important is this trade secret to current or projected revenue?	It is critical to current and/or future revenue and would be nearly impossible to replace	It is important but we are sufficiently diverse that we could make up the difference if pressed to do so	Not very important or we haven't determined its importance

"Medium" and "High" were calibrated for each category (assessing, for example, the relative reputation cost of a "High" impact in the first column vs. a "Medium" impact) and then the overall asset scores combined. This exercise results in a ranked analysis of ABC's trade secrets by relative value, wherein higher scores are associated with trade secrets that are deemed more important or valuable than other trade secrets in ABC's portfolio. Deciding how appropriately to allocate resources to protect assets is not only dependent upon the relative score, but also an assessment of the economic impact should that trade secret be stolen. Accordingly, ABC's Compliance Counsel decides to proceed to the next level of the framework to assess the economic impact of a trade secret theft event for the ten trade secrets that ranked highest in this exercise.

Level 4: Economic Impact Attributable to Trade Secret Theft

In this Level, management will seek to assess the economic impact of a trade secret theft event for the company's most valuable trade secrets identified in Level 3. Applying both quantitative and qualitative analyses, management will calculate the potential economic losses attributable to theft and, leveraging results from previous Levels, adjust the economic loss analysis based on the perceived threat.

4.1: Impact Assessment

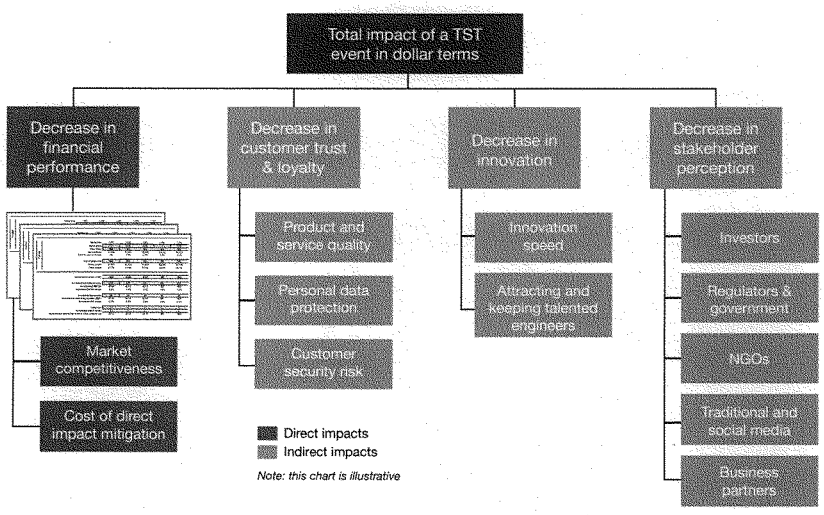
In this step, the company determines the adverse economic impact to the company if an individual trade secret asset is misappropriated. This process enables management to segment the total impact into manageable building blocks and understanding of both direct and indirect impacts helps to establish a complete picture of the economic losses attributable to a trade secret theft event.

- ***Direct Impact:*** A measure of the direct financial and economic losses attributable to a trade secret theft event—i.e., lost sales/revenues, lost market share, lost profits, and/or lost economic opportunity; and
- ***Indirect Impact:*** An assessment of the indirect factors impacting a company's short/long-term ability to compete in the marketplace due to the theft of the output of its investment—e.g., reduction in customer trust due to concerns about ongoing relationships or adverse press impacting the company's reputation in the marketplace.

In this context, it is important to consider both the direct and indirect aspects of a trade secret theft event to help companies capture the full range of economic exposure that threat actors' actions may impose on the organization. The results of the impact assessment provide the basis for establishing a ROI proposition for improving trade secret protection. In most companies, compliance is seen as a cost, not an investment. The valuation is critical to helping companies understand that improving trade secret protection is an investment that has a quantifiable ROI.

In this phase of the framework, ABC's Compliance Counsel may begin by conducting workshops with executives overseeing major subsidiaries or key business units and leaders of core corporate functions (e.g., finance, technology, sales/marketing, human resources) to map areas in which a trade secret theft event could adversely impact the value of the company's operations and business/market environment. A model for these discussions is reflected in Figure 8.

Figure 8: Economic Impact of a Trade Secret Theft (TST) Event



4.1.1: Direct Impact

Estimation of the direct financial impact from the theft of trade secrets is grounded in traditional discounted cash flow analysis that many companies use every day to make business and investment decisions. This estimate typically focuses on various factors including revenues, costs, and profit analysis. It may assess trade secret theft's impact on a company's market competitiveness, or the costs of impact mitigation actions:

- ***Adverse Impact on Market Competitiveness:*** Applying traditional discounted cash flow analysis to estimate the reduction in market share, revenue and profitability due to factors such as business interruption and/or dislocation after a trade secret is stolen, loss of potential licensing revenue, or loss of competitive differentiation; and
- ***Cost of Direct Impact Mitigation Actions:*** After an event, companies may take action to mitigate negative consequences and restore their competitive position or reputation in the marketplace (e.g., litigation against the responsible party). The costs associated with these actions should be included in this element of the estimate.

ABC's management identifies a range of threats related to potential exposure of particular trade secrets. Examples include, but are not limited to, the following:

- *A competitor could steal ABC's source code to re-engineer a product, discount its prices and still generate a profit because it would not have to cover the return on R&D efforts. Based on a market analysis, management can estimate what level of market share, revenues and profit would be lost.*
- *If threat actors compromise the production server for a key service that generates business through continuous micro transactions, the server can go down. Until the company restores operations it would lose revenues. The customer service department would likely work overtime to manage client complaints, and the company might need to prepare and deliver messaging related to the disruption. Management could estimate these lost revenues and additional expenses.*
- *If threat actors hack ABC's servers and gain access to "sensitive business information" related to ABC's supply chain that compromises the supply chain's ability to compete in the marketplace, suppliers could decide to take legal action against ABC if it appears ABC acted negligently in handling suppliers' trade secrets. Such legal action could contribute to increased legal fees and associated costs for ABC. ABC's legal department could make a reasonable estimate of the nature and amount of these costs.*

Applying these concepts, ABC management estimates the direct financial impacts for the top ten trade secrets in its portfolio identified in the Level 1 exercise.

4.1.2: Indirect Impact

Companies must also consider longer-term, indirect adverse changes to their business environment resulting from trade secret theft. As noted above, these issues typically involve qualitative but nonetheless critical impacts to the organization (e.g., customer relationships, reputational matters) that can be thought of as key drivers of company value. The common element of these indirect impacts is that they are strategically important for the company, but the extent to which they drive financial performance is typically difficult to quantify.

In this context, ABC identified several areas in which a trade secret theft event will adversely impact their business.

- ***Customer Trust and Loyalty:*** *ABC believes a trade secret theft event would negatively impact the trust and loyalty the company experiences with certain customers who value the company for product quality and safety. If ABC cannot protect its own assets, customers may doubt that their own confidential information (e.g., design specs) is adequately protected. Customers may express further concerns about a threat actors' ability to access their own systems through the compromised source code. Such factors may decrease customer's willingness to engage with ABC, thereby reducing long-term revenues and profitability.*

- ***Innovation and Talent:*** *ABC's key competitive advantage lies in its innovative approaches and its ability to develop new alternative energy solutions that provide value to customers. If source code is stolen, the company's pace of innovation may stall as enhanced security measures are adopted, requiring engineers to adapt to new policies and procedures. Key engineers may leave the company, or it could become more difficult to recruit new talent. Further innovation processes may be cut back. Collectively, these factors could lead to decreased innovation and subsequent reductions in long term performance.*
- ***Stakeholder Perception:*** *ABC works with multiple stakeholders who influence markets and customers, so maintaining the trust of the company's stakeholders in ABC's security protocols is essential. For example, investors may assert that the company lacks appropriate controls and protection processes to support sustainable growth, deciding to sell shares despite the absence of direct financial consequences of the theft. Also, if discussion of the theft trends on social media blogs or is covered by traditional media, it can influence long-term customers' buying decisions. Similarly, the theft may erode the trust of the company's key business partners.*

Such indirect impact areas all bear upon areas of strategic importance for the long-term performance of companies. To facilitate assessment, companies can consider Key Performance Indicators ("KPI") for each identified indirect impact area and convert them into dollar terms using Multi-Attribute Utility Analysis ("MUA") to measure the economic impact on the business. Specialists familiar with the identified indirect impact areas can inventory existing KPIs and/or create new KPIs to measure performance. While the values generated do not represent accountancy measures, indirect impacts can be converted to economic costs, allowing comparisons of prioritized trade secrets' direct and indirect impacts. This will also help measure the benefits of potential actions companies could take to protect their trade secrets further, as discussed later in the paper.

For example, ABC may convene discussions to identify KPIs across all the identified indirect elements. The company's customer surveys and market surveys targeting future customers include questions that focus on customer trust and loyalty. Management estimates how these survey results would change in case of a trade secret theft event for each of the prioritized trade secrets. With these measures available, MUA techniques enable ABC management to construct a model expressing the economic costs of each KPI, making it comparable to the direct financial impact estimate.

4.2: Threat Adjusted Economic Impact

The Impact Assessment (Level 4.1), Threat Actor Analysis (Level 2.1), and Vulnerability Analysis (Level 2.2) are aligned to form a total "Threat Adjusted Economic Impact" value for each trade secret and across the portfolio. Collectively, these considerations inform management of the potential threats facing individual trade secrets with a clear view of where the impacts would be, how likely a threat is, and how protected the company is against them. This information enables management to allocate resources across the portfolio to adequately safeguard these important assets – the next level in the framework

For example, an important trade secret in ABC's portfolio is inherently valuable to the company, but the threat actor analysis indicated that marketplace demand among threat actors for this trade secret was low and the company's existing procedures and internal control were adequate to mitigate potential exposure. Conversely, ABC's management determines its source code is equally valuable, yet its exposure to threat actors would inflict significant economic harm to the company. ABC's analysis further indicates that new working practices and internal controls would enhance ABC's ability to mitigate potential threats in this area.

Level 5: Protective Action Portfolio Management and Allocation of Resources

Analysis of the Threat Adjusted Economic Impact for those trade secrets deemed most important to a company enables management to make informed decisions about how appropriately to use its existing resources to strengthen its ability to mitigate potential threats through advanced protective measures. With insights into the economic costs of a potential trade secret theft event in hand, management can effectively assess the incremental costs of developing and implementing a trade secret protection management system. This can include including new policies,

procedures and/or internal controls against the perceived threat, and the appropriate allocation of resources. For example, the benefit of new protective actions (e.g., impact mitigation, reduced exposure to threat actors, strengthened access controls) can be measured through the reduction in the Threat Adjusted Economic Impact for a single trade secret or across the portfolio, if the benefit extends to multiple trade secrets. Collectively, this approach enables management to effectively analyze its existing resources and efficiently reallocate those resources to safeguard the company's most important assets; in turn, aligning resources with the company's broader strategic priorities and objectives. The cost of developing and implementing a trade secret protection management system can also be established, thus allowing the company to assess the ROI.

ABC, after completing the previous levels of the framework, has a clearer understanding of which trade secrets are at highest risk of exposure, and how exposure would impact its operations. Now, through a series of workshops with subject matter experts, management lists a series of action items that various parts of the organization planned to protect the selected trade secrets. Some of the identified actions focus on the following areas:

- *IT would raise the company's protection level by establishing new servers and firewalls and ensuring all software is routinely updated;*
- *The product development teams would develop multiple plans to segregate and limit access to source code in order to mitigate the adverse economic impact if one piece of source code were stolen;*
- *The public relations and customer service teams would design "emergency" protocols with which the company can quickly react and communicate to the market and key stakeholders in case of a trade secret theft event. Such a response would help mitigate adverse changes to customer trust and perception of key stakeholders.*

In this process, ABC's management team evaluated the recommendations for advanced protective measures around each of the trade secrets and, within its pool of available resources (e.g., budget, talent/personnel, and capabilities of existing information technology systems), targeted mitigation strategies where the enhanced protective measures would lead to the highest reduction to an individual trade secret's Threat Adjusted Economic Impact. This enabled the company to measure the ROI on each action and select the appropriate portfolio of actions to increase the ROI given the company's available budget.

On this basis, management constructed a briefing to senior executives and ABC's Board of Directors to convey their observations of ABC's trade secret portfolio, potential threat actors targeting the company and exposures identified in the vulnerability analysis. The briefing included recommendations to mitigate these emerging threats, including an improved trade secret protection management system, consisting of new policies, more effective procedures and infrastructure-hardening controls. The recommendations were grounded in an economic assessment that balances incremental costs against expected returns. ABC's management plans to perform this analysis annually to help to establish that the company's compliance and security efforts align with the changing market environment and evolving strategic priorities of the company.

This framework addresses the key components of a company's strategy to protect its trade secrets—identification of the secrets, clarification of where and how they are stored or protected, and informing management's ability to make effective and efficient decisions on how to adequately deploy protection measures based on meaningful economic analyses. Applying this framework is a significant undertaking for any company, particularly those approaching these processes for the first time. Stratifying the framework into discrete levels allows companies to take an iterative approach to safeguarding their trade secrets, in order to marshal the necessary resources, obtain buy-in from key stakeholders, evaluate progress, and gain consensus at each level before continuing. Completing each level should be considered significant progress for any company that undertakes this effort.

How do Expectations of Future Trade Secret Loss Impact Private Sector Decision-Making Today?

Corporate executives around the world regularly make decisions based on expectations about the future. Choices related to new product launches, expanding strategic business relationships, investment in capital projects, and research and development expenditures are each grounded, in part, on companies' expectations about the future. Effective management of a company's trade secret portfolio requires a similar perspective.

- Will the identified trade secret provide the company with a competitive advantage in the marketplace? For how long? What level of economic returns will these trade secrets provide? Over what period of time? How will the company capitalize on this investment in the marketplace?
- How will the company protect these trade secrets from internal and external threat actors to promote the anticipated competitive advantages and returns in the marketplace are achieved? Are new compliance and security protocols required to safeguard the investment during this phase? What is the plan to improve the maturity of the trade secret protection management system and the information security program? How are those costs factored into the expected economic returns?
- How will expectations involving external factors—regulation, openness of the Internet, cybersecurity threats, emerging threat actors in the marketplace, the pace of innovation—drive the company to evaluate the diversity of threats and incremental costs associated with protecting its trade secrets? How can improved trade secret and IP protection be used as a competitive advantage in the global marketplace in attracting customers, partners and investors?

For years, executives have asked questions like these as part of their internal analysis and due diligence around new investments in R&D projects where the investment's expected time horizon for a return extends for several years. In today's marketplace, however, these questions are increasingly important given the emerging threat of trade secret theft and the prevalence of other forms of economic crime that can adversely impact the economic analyses upon which these investments are based. Accordingly, corporate executives are increasingly focused on analyzing potential future scenarios and the consequences of acting (or choosing not to act) to further protect the development of their trade secrets; especially for significant capital investments with extended periods before economic returns are generated.

In 2013, the U.S. Intellectual Property Enforcement Coordinator wrote in its strategic plan on IP enforcement that, "As we move forward, we are aware that new technologies, evolving social norms, new business models, and novel global distribution mechanisms will present new challenges and opportunities to combat infringement of American intellectual property rights."[39]

New challenges and opportunities form the basis of the following section of the report. We modeled three scenarios focused on trade secret protection-related issues over the next 10-15 years. The scenario models are not predictions; but rather projections of possible outcomes based on a narrow combination of drivers. They are intended to challenge assumptions and provoke new thinking about this issue and where it might go in the future.

As part of this scenario modeling effort, we convened panels of subject matter experts from leading companies, law firms that focus on patents and trade secret protection, and personnel from think thanks and academic institutions that focus on trade secret theft and global change. These subject matter experts provided insights on the challenges and opportunities for companies to consider in each of the three scenarios. They also offered mileposts and indicators that would be observable in the real world that might indicate one scenario or aspects of one scenario could become more likely than others.

Key takeaways from our modeling sessions include:

1. *Trade secret protection must increasingly focus on external threat actors who may have designs on stealing critical trade secrets and IP.* However, in the present world and going forward, the insider threat will continue to be a dangerously rich source of trade secret loss.
2. *Changing social norms, especially a country's cultural expectations of the degree to which companies must disclose confidential and commercially sensitive information, will significantly impact trade secret protection in the years ahead.* When considering countries for expansion or new market entry, companies may factor how the government and the culture generally treat secrets, as well as the extent and nature of protections the company can expect to receive if its trade secrets are misappropriated.
3. *The openness of the Internet will have a significant impact on how companies develop and protect trade secrets.* If separating or walling off from the Internet becomes politically and socially accepted, we may see some trade secrets—built on an assumption of an open and thoroughly interconnected world—decrease in value.
   - In the latter half of 2013 some multinational corporations and national governments publicly raised the issue of segmenting or walling off parts of their Internet traffic.
4. *Sectors that are able to band together and share threat information concerning trade secret protection will likely fare better than sectors in which participants remain combative and distrustful of peer organizations.*
   - Intra-sector intelligence sharing already pays dividends in some sectors of the economy; more sectors may pursue this collaborative approach in order to better enable trade secret protection in the coming 10-15 years.

Drivers and Scenarios

Numerous drivers and forces will have an impact on trade secret protection in the coming 10-15 years. For our futures section we selected four drivers that will likely impact these futures and that, in different combinations, offer compelling lessons and different visions for us to consider from our current vantage point.

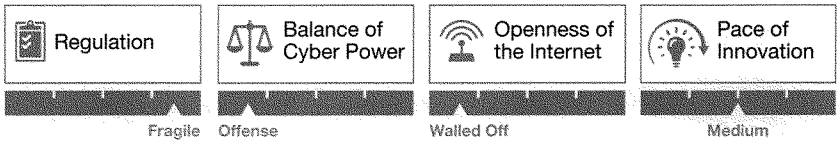
Driver 1: Regulation for the protection of trade secrets: Enhanced global regulation could take hold to increase protection of trade secrets. Alternatively, a future in which no such regulation emerges could be one of increasing collective and individual vulnerability for companies, individuals, countries and other global players.

Driver 2: Balance between cyber offense and defense: A defense-intensive environment would be characterized by its clear, unambiguous ability for attribution of cyber activities and dramatically improved cyber defense systems. A tilt towards the cyber offense would not only mean that threat actors would have the upper hand technologically, but that individuals and companies may be more willing and able to launch cyber attacks on their own.

Driver 3: Openness of cyber commons vs. "walled gardens": The openness of the Internet could remain the status quo for the next 10-15 years. An alternative would be the emergence of walled gardens or the creation of IT networks that are separated from the wider Internet. Walled gardens could be used and created by cities, sectors or countries.

Driver 4: Pace of innovation: The final driver considers the rate at which new ideas are developed and spread across the global economy. Innovation is a key foundation of much of what drives the creation of trade secrets. In futures with a faster pace of innovation, there could more trade secrets.

Scenario 1: "Shelter in the Storm"



In this future, the absence of a robust regulatory framework and international consensus on means for trade secret protection—including but not limited to cybersecurity—combines with offensive cyber capabilities having the upper hand.

Fears of intelligence-gathering by governments, dramatically increased data-theft by criminals, and a series of devastating global cyber attacks creates pressure for individuals and corporations to wall their information off from a dangerous world. In addition to this fear there is a definitive tilt in the balance of cyber power towards those who are on the offense, leading to periodic spikes in cybercrime and cyber-enabled economic espionage. This tilt to the offense is a dual-edged sword, as social norms and the lack of regulation make it easier for some companies, individuals and groups to periodically go on the offensive themselves, launching carefully honed cyber attacks at assessed threat actors.

The perceived dangers to trade secrets and intellectual property on the Internet and connectivity in general lead to new coalitions seeking to increase their security through collective measures. By the end of this 10-15 year period, some companies and sectors have begun to combine forces—sometimes by sector, nation, state or country—behind separate Internet systems that become known as walled gardens.

Information blocs of countries and industries become prevalent. Data centers—formerly globalized—now are owned by groups of countries and hosted in shared locations under the terms of multilateral agreements that exclude non-members.

Eventually, there is some expanded exchange and trade among members of these cyber-blocs. Global commerce decelerates though, and firms with extensive cross-border operations suffer as their ability to conduct data transfers is restricted. Customers prefer to "buy local," reducing firms' need for competition-driven innovation and reducing the value of many trade secrets. Some companies decide to stay outside the walls for a variety of factors.

The observations of many subject matter experts (SMEs) related to this scenario focused on the unique challenge of the walled garden as an active element of this future possibility. SMEs agreed that this world is one of significant adjustment for governments, companies, individuals and even threat actors.

Challenges

- Organizations will face higher costs if they choose to wall off and separate from the open Internet; smaller entities may not be able to survive.
- Global regulations and standards would suffer and be replaced by limited agreements within walled gardens or between walled gardens.
- This world will feature high transaction costs and slower advances in technology.
- Inside the wall, companies will be less agile and will realize fewer gains.
- The high barrier to investment and cooperation outside the walls may lead to lower levels of investment and loss of trade opportunities.
- Being in the walled garden would limit companies' choices of suppliers, employees, service providers and customers.

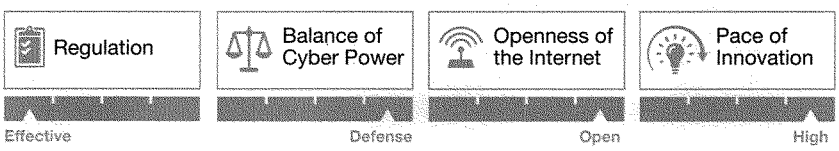
Opportunities:

- Within the gardens, there will be greater security, but at the cost of agility. Those outside the walled gardens will face higher risks, but will also have chances to reap higher rewards.
- Within the walled gardens, especially larger more diverse gardens, there would be numerous opportunities for some sectors to flourish given the high degree of protection from cyber-enabled economic espionage.
- The need to abandon the current model of leveraging overseas talent and distributed supply chains can provide new opportunities for companies to do work that is perceived as more secure though perhaps more costly.
- Companies with a rapid R&D and product development cycle might choose not to wall off, instead remaining in between the walled gardens even if this meant operating at a higher state of risk in order to provide the greatest freedom of movement despite potential increased threats.

Mileposts:

- Quantum computing capabilities to advance the shift of cyber power towards the offense.
- A key member of the G8 or G20 walling off parts of its Internet.
- A series of devastating cyber attacks on trade secrets and IP.
- Governments and companies are unable to gain the advantage on cyber attackers and are constantly behind the curve.

Scenario 2: "The Roaring 20(20s)"



Open cyber commons, combined with a tilt towards stronger cyber defenses, produces a scenario in which companies are increasingly able to protect trade secrets and consequently undertake collaboration, joint ventures, and investment with greater confidence.

Because of the balance of cyber power towards the defense, the private sector at times becomes complacent about security, discounting emerging threats and short-changing security measures. This results in occasional intense bursts of cyber attacks against entire sectors when threat actors find chinks in the technological armor. Public-private partnerships—partly the result of more effective and far-thinking regulation on trade secrets and cyber security—and strong intelligence cooperation within sectors limit such outbreaks to manageable proportions. Companies cooperate to drive a culture of compliance into the global supply chain—upstream and downstream. Trade secret protection management systems are implemented and become as common as quality management systems.

Effective regulation in a defense-intensive environment pushes malicious activity to the fringe and reduces the incentive for criminal efforts to steal trade secrets, while not entirely stopping sophisticated efforts by intelligence services and mature organized criminal networks.

The moderate pace of innovation fosters the creation of new trade secrets and intellectual property. Global trade and commerce steadily progress.

Many SMEs were cautious about the Roaring 20(20s) and were careful to point out that even such a seemingly safe place as this world would come with a cost for many companies.

Challenges:

- Organizations will seek to abuse a stronger regulatory environment by mounting frivolous lawsuits.
- Smaller companies without the resources to deal with new regulation or a harsher litigation environment might be challenged to stay in business.
- The decrease in cyber attacks and a tilt in the balance of cyber power towards the defense may make some companies complacent about security and more vulnerable to attacks from cyber actors and insiders.

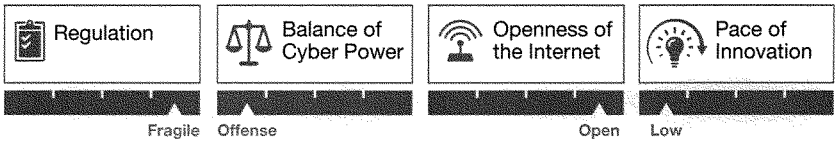
Opportunities:

- If the regulatory regime were truly effective in protecting trade secrets, then the Roaring 20(20s) might witness a golden age of trade secret protection.
- If cyber systems are more secure, companies can focus on policing negative employee behavior, such as the rise of the insider threat. They can continuously improve their trade secret protection management systems.
- Smaller companies may increase their flow of new ideas and trade secrets into larger companies to take advantage of larger companies' regulatory processes and protections.
- Large companies could cooperate to improve respect for trade secrets in their end-to-end supply chains.

Mileposts:

- Significantly increased public outcries about trade secret theft leads to the emergence of a regulatory framework—particularly national-level statutes—that would clearly demonstrate an ability to help companies protect trade secrets.
- Actions by the U.S. Government or other governments to share more clearly defined cyber information and intelligence with the private sector or change laws to enable national-level cyber systems to act as both cyber shield and sword for the private sector, thereby gaining the cyber offensive against threat actors.
- A consistent string of defensive victories against threat actors known to target trade secrets that would be devastating enough to keep them on their heels for extended periods of time.
- Signing and enforcement of global agreements curtailing economic espionage.

Scenario 3: "Radical Transparency"



In this world, regulation and norms on trade secret protection break down, leaving it to individuals and companies to decide when to put up fences, when to steal trade secrets, and when to retaliate for cyber intrusions. The balance tilts in favor of cyber offense, resulting in rapidly emerging threats to trade secrets from individuals and small networks.

Governments can offer little protection other than lip service to the mounting losses. Regulations and customer expectations work to keep corporations or countries from creating walled gardens as an option to protect trade secrets and other IP.

The private sector has little choice other than to adopt an open and transparent collaboration model because widely shared innovation-to-market practices are the norm as the only way to meet customers growing expectation of rapid delivery.

Those launching cyber attacks have the consistent edge in the Radical Transparency world and the high cost of protecting trade secrets disincentives private-sector R&D in some sectors. Some governments try to pick up the slack in R&D in goods and services related to defense, pharmaceuticals, and public health. The effects of slackening R&D are evident only towards the end of the period as the flow of new technologies becomes dramatically slower.

Governments and multinationals exert decreasing influence as "radical transparency" accelerates the power of existing societal forces such as WikiLeaks, grass-roots anti-corruption movements, and new "third forces" gain traction. Transparency advocacy groups' cyber and political power grows and provides them with a platform to pressure companies and governments for transparency above protections for trade secrets.

Many subject matter experts felt that the balance of drivers laid out in this scenario would be the "storm" that might predate the future described in our first scenario, "Shelter in the Storm." Other SMEs opined that this future is, in some ways, not far off from the status quo. Lastly, some SMEs independently concluded that this world would be welcomed by some of the largest Internet-related products and services companies given their interest in openness and transparency.

Challenges:

- For businesses this is a hypercompetitive environment for resources, talent and opportunities.
- Given the hypercompetitive environment smaller firms may not do well in this future.
- Some organizations may seek to act preemptively against perceived threats, and might feel freer to use cyber weapons against known or suspected threat actors.

Opportunities:

- Academic institutions and non-profits, which have long emphasized transparency, would become more influential compared to the present day.
- Given the balance of cyber power and the increasing acceptance of transparency, non-electronic document delivery systems, such as couriers and package delivery companies, might see their services expand for businesses that will not risk electronic networks lest their information might be divulged by those seeking transparency or to steal the information.
- Some companies can band together to share information face-to-face as some sectors have done. The financial sector's creation of the Financial Services Information Sharing and Analysis Center ("FS-ISAC") is a good example of what we might see more of in this future.

Mileposts:

- Organizations that champion transparency gain sponsorship from global leaders or G20 countries, or find champions from leaders of similar stature.
- Use of stolen data becomes more accepted, driven by changes in social norms.
- National and international regulations and treaties on trade secret protection flounder and fail.
- A sustained mass movement against trade secrets or corporate secrecy that gains traction beyond the fringes of political circles.

Key observations from scenario modeling exercise:

Companies and industry associations should consider new and innovative ways to come together to think about the road ahead for trade secret theft, and to identify the drivers that will impact trade secret protection in their areas of concern. The drivers used to construct these three scenarios represent only a fraction of the many influences that will shape how trade secrets are protected and misappropriated in the next 10-15 years. Additional forward-looking analyses that consider how threats to trade secrets may evolve may illuminate other critical drivers. Such efforts will spark debate and discussion about which drivers companies, governments and individuals can influence most effectively in order to create more security and stability for their interests and assets.

Please note that the possible opportunities and challenges summarized in our scenario modeling exercise can be replicated or supplemented by individual companies to help them prepare for a variety of future outcomes and to be ready to act decisively to make the appropriate and most secure use of their intellectual property and trade secrets, regardless of what future emerges. By understanding how trade secret misappropriation and other aspects of trade secret protection, including trade secret protection management systems, may develop in the next decade, companies can incorporate these trends into the framework analysis documented earlier in this study.

Conclusion

The trade secret evaluation methodology provided in this report can provide a first step in a larger collective effort to improve trade secret protection, and help companies to better appreciate the importance of proactive protection as an up-front investment. At the company level, firms would benefit from a better understanding the relative value of their trades secrets and the harm that any loss or theft would inflict on them. Understanding the probability and severity of a potential breach can better inform decisions on investments and other critical activities. We hope this also encourages and inspires companies to be more forthcoming in discussing the challenges associated with trade secret protection, thus advancing a broader dialogue on this issue.

This report also provides a glimpse into three possible futures concerning trade secret theft. In addition to demonstrating the breadth of situations that companies must consider and plan for, such a modeling exercise is particularly critical in an era where technology, policy, customer demand and innovation are making trade secrets ever more valuable to those who create them as well as those who wish to steal them. Companies that fail to anticipate the evolution of threats, regulation and other key drivers risk falling behind their competitors and losing market share.

There is increasing convergence between concepts of privacy and data security generally and trade secret protection. The measures that consumers use to protect their personal information overlap significantly with measures that companies take to protect their trade secrets (e.g., consumers and employees not falling victim to spear-phishing scams; not storing sensitive information in the "cloud"). The more that companies can emphasize that their trade secret protection measures can be used to protect personal privacy, the more acceptances may be gained in employee populations. This may occur on a national level as well as a company level.

The challenge of trade secret theft is too large for any one government, company or organization to deal with alone—only a collective focus on this issue will help improve innovators' ability to secure their most critical information and intellectual property. This cooperative effort will be strongly aided by the investment of individual companies' time and resources to help to establish they know who threatens their own interests and how to measure the value of their own trade secrets. Replication of this sort of increased self-awareness across entire sectors would produce a detailed understanding of the collective threats and challenges, and the thorough extent of the value of trade secrets. Private sector companies—and other targets of trade secret theft—should approach this issue with a sense of urgency. Threat actors show no signs of slowing their attacks on trade secrets, and each new advance in technology brings new potential vulnerabilities with it.

"An environment where it may be easier to steal a vital intangible asset than it is to value, disclose, or even realize its loss is an inherently risky one."

– PwC Global Economic Crime Survey, 2014

Acknowledgements

This report represents the analysis and efforts of many individuals within CREATe.org and PwC. This publication was produced under the direction of Pamela Passman and Leslie Benton from CREATe.org and Sanjay Subramanian and George Prokop from PwC. Our report was created and coordinated by Marissa Michel, Craig Stronberg and Peter Geday.

During the drafting of this report, we consulted with numerous subject matter experts in the private and public sectors who participated in our threat modeling workshops and reviewed our final draft. We also would like to thank Roberto Rojas for his assistance.

Endnotes

1 "Economic Espionage Act of 1996" Published by the U.S. Government

2 Article 39 of the World Trade Organization's Agreement on Trade Related Aspects of Intellectual Property Rights ("TRIPS") states: "Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or Used by others without their consent in a manner contrary to honest commercial practices so long as such information: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret"

3 The Center for Responsible Ethics And Trade ("CREATe.org"), Trade Secret Theft: Managing the Growing Threat in Supply Chains (May 2012)[please add link]

4 "The 2012 Statistical Abstract/National Data Book. Patents and Trademarks: 1990 to 2010," Census. Bureau, U.S. Department of Commerce, 2013

5 "The Report of the Commission on the Theft of American Intellectual Property", 2013

6 "Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods", General Accountability Office, April 2010

7 Ibid

8 National Science Foundation, National Center for Science and Engineering Statistics. 2013. National Patterns of R&D Resources: 2010–11 Data Update.

9 2013 and 2013 Global R&D Funding Forecasts, *Battelle.org* and *R&D Magazine*—December 2012 and December 2013

10 The Battelle Foundation, "2013 Global R&D Funding Forecast," December 2012

11 Justin Hicks and Robert D. Atkinson, "Eroding Our Foundation: Sequestration, R&D, Innovation and U.S. Economic Growth," The Information Technology & Innovation Foundation, September 2012

12 Association of Certified Fraud Examiners ("ACFE"); "Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study"

13 Treasury Inspector General For Tax Administration: Office of Inspections and Evaluations, "The Internal Revenue Service Needs to Improve the Comprehensiveness, Accuracy, Reliability and Timeliness of the Tax Gap Estimate," August 21, 2013

14 Myths and Realities of Governance and Corruption, Daniel Kaufmann, World Bank, October 2005

15 Business Software Alliance, 2012, "The Shadow Market: 2011 BSA Global Software Piracy Study: Ninth Edition"

16 U.S. Department of Justice: The Economic Impact of Illicit Drug Use on American Society, 2011

17 Havocscope: Global Black Market Information; "World Black Market Value", December 2013.

18 Illicit Financial Flows from Developing Countries: 2002-2011. Dev Kar and Brian LeBlanc. Ford Foundation, December 2013

19 Office of the National Counterintelligence Executive ("ONCIX"), "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011", October 2011, published by the Office of the Director of National Intelligence

20 Office of the National Counterintelligence Executive ("ONCIX"), "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011", October 2011, published by the Office of the Director of National Intelligence

21 Ibid

22 Ibid

23 "Chinese National Sentenced to 87 Months in Prison for Economic Espionage and Theft of Trade Secrets," U.S. Department of Justice, December 21, 2011.

24 RJGG v Director General of Security [2013] FCA 269 (Federal Court of Australia, Foster J, 27 Marcy 2013)

25 PwC, State of Cybercrime Survey 2013; State of Cybercrime Survey 2012

26 Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets." February 2013

27 Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets." February 2013

28 Ibid

29 Katherine Herbig, "Allegiance in a Time of Globalization," Defense Personnel Security Research Center, December 2008.

30 Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, February 2013

31 Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, February 2013

32 "White House Strategy to Combat Transnational Organized Crime", The White House, July 19, 2011

33 Organized Crime and Cyber-Crime: Implications for Business, Phil Williams, CERT® Coordination Center

34 Office of the Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence," March 12, 2013

35 Raj Samani and Francois Paget, "Cybercrime Exposed: Cybercrime-as-a-service," McAfee.

36 Dr. Mike McGuire and Samantha Dowling, "Cyber crime: A review of the evidence. Research Report 75. Chapter 1: Cyber-dependent crimes," Published by the United Kingdom Home Office, October 2013

37 Office of the Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence," March 12, 2013

38 Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases, U.S. Attorneys' Bulletin, November 2009

39 U.S. Intellectual Property Enforcement Coordinator, 2013 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT, June 2013. Published by the U.S. Government

www.create.org

www.pwc.com

© 2014 CREATe.org. All Rights Reserved

© 2014 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the U.S. member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

Prepared Statement of Drew Greenblatt

Testimony
of Drew Greenblatt
President and Owner
Marlin Steel Wire Products

"Economic Espionage and Trade Secret Theft:
Are Our Laws Adequate for Today's Threats?"
May 13, 2014

Before the
U.S. Senate Judiciary Committee, Subcommittee on Crime and Terrorism

Chairman Whitehouse, Ranking Member Graham and members of the Subcommittee on Crime and Terrorism, thank you for your focus on the critical challenge of trade secret theft and for the opportunity to testify today.

My name is Drew Greenblatt, and I am the President and owner of Marlin Steel Wire Products LLC (www.marlinwire.com), based in Baltimore, Maryland. Marlin Steel Wire is a leading manufacturer of custom wire baskets, wire forms and precision sheet metal fabrication assemblies – all produced here in America for the aerospace, automotive, medical, and pharmaceutical industries in the United States and 36 other countries around the world. I am here because:

- Trade secrets are vital for manufacturers of all kinds – not just big companies, but also small firms like mine;

- America's trade secrets laws and policies must keep pace with today's threats, which increasingly are interstate and international; and

- Manufacturers need your help to effectively and efficiently protect and enforce trade secrets and to secure strong commitments in our trade agreements.

Like so many other manufacturers, Marlin Steel Wire competes in a global economy. We succeed through investments in ideas and innovations and through the hard work of our dedicated employees. When I bought Marlin Steel Wire Products back in 1998, we were a local business making bagel baskets, with roughly $800,000 in sales and 18 employees. Last year, we had almost $5 million in sales. We now have 24 employees.

Marlin is a proud member of the National Association of Manufacturers (NAM) and the National Alliance for Jobs and Innovation (NAJI). The NAM (www.nam.org) is the largest industrial trade association in the United States, representing more than 12,000 manufacturers large and small in all 50 states. In fact, the average company that NAM represents has between 35 and 40 employees. I serve on the NAM's Board of Directors and its Executive Committee.

I am also the co-founder and chairman of NAJI (http://naji.org), an alliance of 35 business associations and some 380 manufacturers across the country. NAJI works to defend the critical innovative aspects of advanced manufacturing by preventing unfair competition resulting from foreign manufacturers exploiting pirated software and other stolen intellectual property. Both the NAM and NAJI are working hard to strengthen protection of trade secrets and other intellectual property in order to level the playing field for businesses in the United States.

Today, trade secrets are more important than ever to manufacturers small and large. These vital intangible assets include everything from proprietary manufacturing plans, software, processes and formulas to research, marketing data and customer lists. The trade secrets of publicly traded U.S. companies alone are worth an estimated $5 trillion. The knowledge assets of private companies like mine surely add much more to the total.

Small businesses, in particular, rely on trade secrets to protect their innovations, often because they are less expensive to retain and enforce than patents. For Marlin Steel Wire, trade secrets are our intellectual property – our "secret sauce." We leverage the expertise of our employees – 20 percent of whom are mechanical engineers – to manufacture custom-designed products that meet specific customer performance requirements through proprietary processes.

That's why addressing the serious and growing threat of trade secrets theft is so essential. Trade secrets increasingly are at risk in today's mobile and interconnected global marketplace. Estimates of losses from trade secrets theft range from one to three percent of GDP in the United States and other advanced developed economies.[1] The head of the National Security Agency and U.S. Cyber Command believes theft costs American companies $250 billion per year.[2]

In our parents' or grandparents' day, trade secrets often were stolen by individual employees acting alone. They took paper documents and sold them to competitors across town. Now, trade secrets are digital and vulnerable to viruses spread through nefarious websites and hackers operating as part of criminal enterprises. Proprietary information that might once have taken a moving truck to transport can walk out the door on a thumb drive and be sold to governments or competitors across the coutnry or half a world away.

Trade secret theft is increasingly international in scope. As documented in recent reports by the Office of the National Counterintelligence Executive[3] and the Defense Security Service,[4] foreign governments like China and Russia are working

---

[1] Center for Responsible Enterprise and Trade and PWC, "Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats," February 2014.
[2] Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *Foreign Policy*, July 9, 2012.
[3] Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," October 2011.
[4] Defense Security Service, "Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting," 2013.

systematically to access the trade secrets of businesses in the United States and many other countries. Through cyber incursions, they are targeting and stealing advanced manufacturing and other technologies.

Trade secrets are acquired and developed through many years of company experience and investment. They provide a powerful business advantage in highly competitive sectors like manufacturing – but only as long as they remain confidential. Trade secrets are not exclusive rights. Once disclosed, their value is lost forever. Theft has a real, measurable, real-world impact. It costs good-paying U.S. jobs and can even put entire businesses at risk.

Cyber incursions not only threaten proprietary information, but also our people and products. Today, the lasers, robots and other machinery that drive advanced manufacturing are all connected to networks. At Marlin Steel Wire, we are safety nuts. Our plant has worked 1,975+ days without a lost time accident. But if hackers interfere with our machinery, they can put the safety of our workers at risk and destroy production runs. We can't let that happen.

That's why we are doing everything we can to harden our networks and safeguard our trade secrets. At Marlin Steel Wire, we protect trade secrets through non-disclosure contracts and technological security measures. We educate our employees about the importance of protecting proprietary information and the potential business impact if trade secrets are stolen or disclosed. Those measures are costly, but unfortunately all too necessary. For the amount I spend on security, I could hire another full-time welder. There are a lot of unemployed welders in Baltimore.

But there is only so much Marlin Steel Wire and other companies can do alone. Congress and the Administration have critical roles to play in ensuring America's laws, policies and law enforcement actions are equal to today's threats. The good news is that Washington is recognizing the problem. Congress has introduced and passed

legislation that is helping to upgrade our nation's laws for the 21st century. The White House has organized federal agencies behind a strategy to mitigate trade secret theft.[5]

The FBI has increased criminal enforcement of trade secret theft, conducting more investigations. The Foreign and Economic Espionage Penalty Enforcement Act, passed by both houses of Congress and signed in to law last year, went a long way to putting deterrent penalties in place. But that's not enough. We need to step up our game. Congress and the Administration must prioritize three actions that can raise the stakes for criminals, hit thieves in their wallets and better enable businesses to protect and enforce their rights.

First, we need strong operational collaboration between federal agencies as well as more engagement between those agencies and the business community. Protecting and enforcing trade secrets can't be the job of just one agency – a silo approach to a broad problem. We need a comprehensive, integrated push. The FBI, Justice, Customs and other agencies must work together to increase investigations and prosecutions, track down illicit gains and deliver real-time information to businesses about cyber threats and how to respond.

Second, we need access to federal civil enforcement for trade secrets theft, which well-conceived legislation like the Defend Trade Secrets Act recently introduced by Senators Chris Coons (D-DE) and Orrin Hatch (R-UT) would provide. Despite their strategic economic importance, trade secrets misappropriation is the only form of U.S. intellectual property violation for which the owner lacks access to federal court. This leaves U.S. firms without a key tool to prevent trade secret theft and recover any losses.

Access to federal courts is critical for businesses of all kinds. State civil trade secret laws alone often are not sufficient to deter and remedy interstate theft. State courts are not always well suited to working quickly across state and national

[5] Office of the Intellectual Property Enforcement Coordinator, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," February 2013.

boundaries to facilitate discovery, serve defendants or witnesses, or prevent a party from leaving the country. State laws can vary, making it harder for firms to craft consistent policies.

When a trade secret is stolen, its owner must act quickly to protect proprietary information and preserve evidence. Without access to federal courts, thieves have the advantage. For example, there are at least six airports with international flights within a two-hour drive from my facility in Baltimore. Five of those airports are in other states – New Jersey, Pennsylvania and Virginia. By the time multiple state courts take action, the criminals will be long gone.

Beyond any delays, taking civil action to protect trade secrets across multiple jurisdictions is also difficult and costly, particularly for small businesses. Unless small businesses have legal firms on retainer in different states, which most do not have, of course, they are effectively barred from using a key tool to defend their rights. That needs to change, and I urge the Judiciary Committee to act swiftly on legislation providing access to federal courts for trade secret theft.

Finally, we must meet the global challenge of trade secrets theft with global solutions. The United States should make common cause with Europe, Japan and others around the world that are facing the same problems and beginning to pursue their own solutions. We need strong trade secret protection and enforcement commitments in America's trade agreements, including those under negotiation with Europe and 11 Pacific Rim nations.

With effective criminal protection and access to federal civil enforcement here at home, U.S. negotiators can work with our overseas partners to improve trade secret protection and enforcement and to foster collective action through our trade agreements. Our partners have a shared stake in the success of that endeavor. They should be eager to work with us and to contribute ideas and solutions from their own experience.

* * * * *

Chairman Whitehouse, Ranking Member Graham and members of the Subcommittee, trade secrets are vital for manufacturers small and large. America's trade secrets laws and policies much keep pace with today's threats. Manufacturers need your help to ensure they can effectively and efficiently protect and enforce their trade secrets.

I applaud your attention to this critical challenge and your focus on solutions. With strong global partnerships, with closer collaboration between federal agencies and between government and business, and with improvements to U.S. laws, including access to federal civil enforcement, we can have a real impact.

Thank you for the opportunity to testify this afternoon. I look forward to answering any questions you may have.

PREPARED STATEMENT OF DOUGLAS K. NORMAN

Hearing on

**"Economic Espionage and Trade Secret Theft:
Are Our Laws Adequate for Today's Threats?"**

**United States Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism**

May 13, 2014

**Written Statement of Douglas K. Norman
Vice President and General Patent Counsel
Eli Lilly and Company**

Testimony of Douglas K. Norman
Vice President and General Patent Counsel
Eli Lilly and Company
"Economic Espionage and Trade Secret Theft:
Are Our Laws Adequate for Today's Threats?"
May 13, 2014

Good afternoon Chairman Whitehouse, Ranking Member Graham, and Members of the Committee. My name is Doug Norman. I am the Vice President and General Patent Counsel of Eli Lilly and Company. Thank you for the opportunity to testify today on an issue of great importance not only to my company — and not only to my industry — but to all segments of the American economy.

I have held leadership positions in the intellectual property field for many years, including serving as President of the Intellectual Property Owners Association and leading various IP committees, including with the National Association of Manufacturers and the Pharmaceutical Research and Manufacturers of America. Eli Lilly and Company was founded and is headquartered in Indianapolis, Indiana. On May 10th – just last Saturday – Lilly celebrated its 138th birthday as a U.S. company. Our mission at Lilly is to discover and develop medicines that help people live longer, healthier and more active lives. Our major areas of innovation include therapies for cancer, diabetes and mental illnesses. To fulfill this vision, Lilly must rely upon intellectual property protection that includes patents, trademarks and trade secrets. Unfortunately, like too many of America's leading innovator firms, Lilly has recently been the victim of trade secret theft.

Eli Lilly is a member of the Protect Trade Secrets Coalition, a cross-sector group of companies that are working to protect and defend trade secret property by supporting a harmonized, federal civil remedy for trade secret misappropriation.[1] We are pleased to support the Defend Trade Secrets Act, S. 2267, which would accomplish this objective, and thank Senators Coons and Hatch for introducing it.

We also are encouraged by your work, Chairman Whitehouse and Ranking Member Graham, to ensure law enforcement has the tools it needs to prosecute trade secret theft; and we appreciate the effort by Senator Flake to highlight the continued problem of trade secret theft that occurs abroad.

We also appreciate the leadership that Chairman Leahy and Ranking Member Grassley have demonstrated on trade secret protection. The bipartisan interest in improving trade secret law evidenced by this Committee's work is important to our shared objective of improving the effectiveness and efficiency of remedies for trade secret misappropriation. Likewise, we are

---

[1] The Protect Trade Secrets Coalition comprises Abbott Laboratories, Caterpillar, Corning Incorporated, Eli Lilly and Company, General Electric, Medtronic, Micron, Microsoft, Monsanto, NIKE, Philips, The Procter & Gamble Company, and United Technologies Corporation.

heartened by the discussions we have had with the leadership and Members of the House Judiciary Committee, and we look forward to working with them on this issue that is so important to all segments of our economy.

The Importance of Trade Secrets.

Trade secrets are an essential form of intellectual property and part of the backbone of our information-based economy. Trade secrets are critical for the competitiveness of American companies in the 21st century. The information trade secret law protects is diverse, including manufacturing processes, industrial techniques, formulas, or customer lists. While companies rely on patent or copyright protection for some inventions and innovations, increasingly our competitiveness rests on protecting our trade secrets.

Whether you are a major pharmaceutical company like Eli Lilly or a start-up software company, your trade secrets are a big part of what sets you apart in the marketplace, and their protection is vitally important to maintaining a competitive edge and keeping workers on the job. Innovative companies have led the world in creating products that change how we work, play, communicate, create, and live our lives. Trade secret protection is a critical component of this innovation. By better protecting trade secrets, Congress can help create an environment conducive to fueling the next generation of new products and processes and the employment opportunities that flow from innovation.

Unfortunately, this form of information and know-how is particularly vulnerable to misappropriation given the rapid technological advances that have resulted in greater connectivity, as well as more globalized supply chains and more mobile employees.

The Vulnerability of Trade Secrets.

Companies that are creating jobs in America are also increasingly the targets of sophisticated efforts to steal proprietary information, harming our global competitiveness. Broad industry surveys have found that 60 percent of companies surveyed from diverse industries had detected attempted or actual trade secret theft in a given year. Many such attacks go undetected. Most of the stolen trade secrets were located in the United States, but the major beneficiaries of the theft were foreign entities.

A theft can come through cyber-attack, voluntary or involuntary disclosure by an employee, or misappropriation by a joint venture partner. Often the theft is state-sponsored. Government sources have estimated that the loss of intellectual property for American companies from cyber espionage is $200 billion to $300 billion per year.

The Need to Modernize Trade Secret Laws.

The tools thieves use in their attempts to steal American trade secrets are growing more sophisticated by the day. Our law must keep pace. The current legal tools available to prevent trade secret theft are antiquated and inconsistent with the robust protection available in other areas of intellectual property law. In the United States, these tools include a federal criminal

law, the Economic Espionage Act of 1996 ("EEA"), and an array of state laws that provide civil relief.

Under the EEA, it is a federal crime to misappropriate trade secrets for the benefit of a foreign government or for economic gain. The Act is an insufficient remedy, however, because it is solely a criminal statute. Criminal law to protect intellectual property has two important limitations. First, the FBI and the Department of Justice have limited resources and would never be in a position to bring charges in all cases of interstate trade secret theft. Second, criminal law punishes the defendant, but the process for compensating the victim is unwieldy, particularly when compared to relief available under civil law. For these reasons, federal statutes provide owners of other intellectual property — patents, copyrights, and trademarks — with the right to bring a civil action in federal court to recover damages and, in appropriate cases, enjoin further infringement.

State laws provide trade secret owners with a civil remedy the owner can bring against a party that has misappropriated a trade secret. State trade secret laws developed and made sense at a time when misappropriation was largely a local matter. It works well, for instance, when an employee of a local business steals a customer list and takes it to the business down the street. But for companies that operate across state lines and have their trade secrets threatened by competitors around the globe, the array of state laws is inefficient and inadequate for several reasons.

First, companies need compliance plans to protect their trade secrets. Under the array of state laws, a company that operates in more than one state bears significant additional and unnecessary costs to protect this critical form of intellectual property. The company must investigate the different requirements of different state laws, making it difficult to craft an effective and uniform national compliance plan. For small companies these costs can be prohibitive and take up precious resources that would otherwise be used to support innovation.

Second, trade secret theft today is increasingly likely to involve the movement of the secret across state lines. Such multi-jurisdictional movement makes discovery and service of process difficult. While federal courts permit subpoenas to be issued nationwide, state courts are often not as efficient at obtaining discovery in other states.

Third, trade secret cases require swift action by courts across state lines to preserve evidence and protect the trade secret from being divulged. This is particularly true when the theft is by an individual looking to flee the country, as is increasingly the case. State courts lack the ability of the federal system to serve defendants and prevent the disclosure of the trade secret or destruction of evidence. Once the trade secret has been divulged, or is made known to a competitor, trade secret protection may be lost forever and the harm from disclosure is often irreparable.

Support for the Defend Trade Secrets Act.

We were pleased to announce our support for the Defend Trade Secrets Act along with more than 30 companies and associations from all segments of our economy. The breadth of

support for the legislation — from companies focused on diverse areas such as software, biotech, semiconductors, medical devices, agriculture, and apparel — demonstrates the importance of a harmonized, federal civil remedy. The companies that have already indicated their support for S. 2267 often disagree on other areas of intellectual property protection, but we are united in this effort.

We support the Defend Trade Secrets Act because it will create a uniform federal civil remedy for trade secret misappropriation and provide a mechanism to obtain expedited relief when there is a threat that our stolen secrets are about to be disclosed or the evidence destroyed.

The consistent, harmonized legal framework that S. 2267 establishes will provide a more efficient and effective legal structure to protect our property. It also puts trade secret protection in-line with the remedies available for owners of other forms of intellectual property. Further, by creating a uniform standard, the legislation will encourage companies to create one set of best practices to protect their trade secrets in every state.

We appreciate the leadership Senator Coons and Senator Hatch have shown with this legislation.

We also look forward to working with Chairman Whitehouse and Ranking Member Graham on ensuring law enforcement has the tools it needs to prosecute trade secret theft. Similarly, we look forward to working with Senator Flake on his initiative to fight theft that occurs overseas. While we want to be careful not to encourage other countries to pass laws targeting conduct that occurs purely in the United States, we agree that it is important to study ways in which we can address this form of theft effectively.

Conclusion.

Americans have a long history of investing in innovation. American companies are competing globally and the know-how resulting from those investments is constantly under attack from sources both foreign and domestic. A national solution that provides consistent and predictable trade secret protection and enforcement is therefore essential to our global competitiveness. Now is the time for Congress to enact the same type of legal protections for trade secrets that other forms of intellectual property – including patents, trademarks and copyrights – have long enjoyed. The Defend Trade Secrets Act will establish the gold standard for national trade secret laws globally and serve as an important base for international harmonization efforts. We urge the Committee to consider this legislation and for all Senators to support it.

QUESTIONS SUBMITTED TO RANDALL C. COLEMAN BY SENATOR WHITEHOUSE

Questions for the Record
"Economic Espionage and Trade Secret Theft:
Are Our Laws Adequate for Today's Threats?"
May 13, 2014
Senator Sheldon Whitehouse

Randall C. Coleman:

As we discussed, multiple units within the FBI are responsible for economic espionage and trade secret theft cases.

1. Please explain the division of responsibility for these cases within the Bureau, and specifically the roles of the Counterintelligence, Cyber, and Criminal Investigative Divisions.
2. How and on what basis is the determination made as to where a case is assigned?
3. What efforts are made and what procedures are in place to ensure that agents in all relevant divisions are sharing information and communicating with each other on a regular basis?
4. Has the FBI considered consolidating responsibility for these cases within one unit, and for how long does the FBI think this will remain a sensible division of responsibilities?

QUESTIONS SUBMITTED TO PETER L. HOFFMAN BY SENATOR FLAKE

Written Questions of Senator Jeff Flake
U.S. Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism
Hearing: Economic Espionage and Trade Secret Theft
May 20, 2014

Peter L. Hoffman, Vice President, Intellectual Property Management, The Boeing Company

1. Do you agree that both domestic and foreign misappropriation of trade secrets is a growing and persistent problem?

2. Do you support legislation that would provide additional tools to protect companies against domestic and foreign trade secret theft?

QUESTIONS SUBMITTED TO DOUGLAS K. NORMAN BY SENATOR FLAKE

Written Questions of Senator Jeff Flake
U.S. Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism
Hearing: Economic Espionage and Trade Secret Theft
May 20, 2014

Douglas K. Norman, Vice President and General Patent Counsel, Eli Lilly and Company

1. Do you agree that both domestic and foreign misappropriation of trade secrets is a growing and persistent problem?

2. Do you support legislation that would provide additional tools to protect companies against domestic and foreign trade secret theft?

QUESTIONS SUBMITTED TO PAMELA PASSMAN BY SENATOR FLAKE

Written Questions of Senator Jeff Flake
U.S. Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism
Hearing: Economic Espionage and Trade Secret Theft
May 20, 2014

Pamela Passman, President and Chief Executive Officer, Center for Responsible Enterprise and Trade

1. Do you agree that both domestic and foreign misappropriation of trade secrets is a growing and persistent problem?

2. Do you support legislation that would provide additional tools to protect companies against domestic and foreign trade secret theft?

RESPONSES OF RANDALL C. COLEMAN TO QUESTIONS SUBMITTED BY SENATOR WHITEHOUSE

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 11, 2014

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Randall C. Coleman, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, before the Committee on May 13, 2014, at a hearing entitled: "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?" We apologize for our delay in responding to this request.

Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

Peter J. Kadzik
Assistant Attorney General

Enclosure

cc: The Honorable Charles E. Grassley
Ranking Member

Responses of the Federal Bureau of Investigation to Questions for the Record Arising from the May 13, 2014, Hearing Before the Senate Committee on the Judiciary Subcommittee on Crime and Terrorism Regarding "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?"

Questions Posed by Senator Whitehouse

As we discussed, multiple units within the FBI are responsible for economic espionage and trade secret theft cases.

1. Please explain the division of responsibility for these cases within the Bureau, and specifically the roles of the Counterintelligence, Cyber, and Criminal Investigative Divisions.

Response:

Because the theft of trade secrets can involve a range of activities and circumstances, three programs in the FBI share the responsibility for investigating these violations. When the FBI learns of a possible trade secret theft, we assess the available information to determine whether the theft resulted from an insider or a cyber intrusion. If the theft resulted from a cyber intrusion and there is no insider nexus, the Cyber Division provides program management for the investigation. If the trade secret theft appears to be the work of an insider and there is a possible foreign nexus, the investigation is managed by our Counterintelligence Division; if theft by an insider does not appear to have a foreign nexus, it is managed by the Financial Institution Fraud Unit in the Criminal Investigative Division.

2. How and on what basis is the determination made as to where a case is assigned?

Response:

Please see the response to Question 1, above.

3. What efforts are made and what procedures are in place to ensure that agents in all relevant divisions are sharing information and communicating with each other on a regular basis?

Response:

The FBI is constantly working to ensure that information is shared across divisions and that resources are used efficiently. Strategic analysts are embedded in each operational division at FBI Headquarters. These analysts are led by an Intelligence Deputy Assistant Director (DAD) who reports to the FBI's Directorate of Intelligence (DI). To ensure the cross-programmatic sharing of information, the DI has developed a standardized framework for collecting, reporting, and disseminating intelligence. Within the operational divisions, threat-based fusion cells now serve as intelligence teams to integrate all aspects of the intelligence cycle, providing a more strategic and nimble approach to identifying and mitigating current and emerging threats and facilitating more seamless information sharing among Intelligence Analysis and Special Agents across programs. Each fusion cell reports to its program's Intelligence DAD, and these DADs meet monthly to ensure close collaboration.

4. Has the FBI considered consolidating responsibility for these cases within one unit, and for how long does the FBI think this will remain a sensible division of responsibilities?

Response:

The FBI's DI ensures that the intelligence elements embedded in our operational divisions communicate effectively in order to ensure a cross-programmatic approach to threats. As noted above, the theft of trade secrets can involve a range of activities and circumstances. The FBI believes the delineation of responsibilities discussed in response to Question 1 is the most effective use of our resources because it allows us to leverage the subject matter expertise offered by each program to address the particular activities and circumstances involved in a given case. As we have in the past, we will continue to evaluate our organizational structure and business processes to ensure we are best positioned to address the evolving threat.

RESPONSES OF PETER L. HOFFMAN TO QUESTIONS SUBMITTED BY SENATOR FLAKE

Questions for the Record
Peter L. Hoffman
Vice President, Intellectual Property Management, The Boeing Company

Senate Judiciary Committee Subcommittee on Crime and Terrorism
"Economic Espionage and Trade Secret Theft:
Are Our Laws Adequate for Today's Threats?"
May 13, 2014

QUESTIONS POSED BY SENATOR FLAKE

Question 1. Do you agree that both domestic and foreign misappropriation of trade secrets is a growing and persistent problem?

Answer: Yes, both domestic and foreign misappropriation of trade secrets is a growing and persistent problem. In February of 2013, the White House issued the Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, which concluded that the pace of economic espionage and trade secret theft against U.S. corporations is accelerating and moving to the cyber world. Because online attacks are hard to detect, allow access to more information at once, and are difficult to attribute, in its 2011 report to Congress, the Office of the National Counterintelligence Executive predicts that cyber intrusions will become the preferred method for trade secret theft. We appreciate your bringing attention to the fact that many of these stolen files are destined for competitors located outside of the U.S., and the difficulties U.S. companies face as a result. We are also thankful that the Committee is considering legislation to address trade secret misappropriation on a bipartisan basis, and we look forward to working with you to strengthen our trade secret laws.

Question 2. Do you support legislation that would provide additional tools to protect companies against domestic and foreign trade secret theft?

Answer: Yes, Boeing supports legislation that would provide additional tools to protect companies against domestic and foreign trade secret theft. Trade secret laws are vital to protecting Boeing's substantial intellectual property. Theft of trade secrets hurts more than just the victim companies. When stolen trade secrets are taken overseas, it hurts the U.S. economy and will likely cost American jobs. U.S. companies need the ability to take immediate action in a United States federal court to quickly contain an escape of our trade secrets here before we are harmed by their disclosure in the U.S. or elsewhere. As to foreign theft, we hope that any new laws enacted would raise awareness of the issue, promote cooperation between U.S. and foreign law enforcement, and empower our trade negotiators to encourage our trading partners to similarly raise the bar. Boeing supports strengthening our trade secret protections, so long as any new law provides an effective and efficient means of securing our valuable trade secrets, while being narrowly tailored to prevent a reasonable likelihood of abuse or overreach in its application.

RESPONSES OF DOUGLAS K. NORMAN TO QUESTIONS SUBMITTED BY SENATOR FLAKE

Hearing on "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?"

Questions for the Record from Senator Flake for Douglas K. Norman

Question 1. Do you agree that both domestic and foreign misappropriation of trade secrets is a growing and persistent problem?

Answer: I agree. Trade secret misappropriation is an increasing problem in the United States and around the world.

Trade secret protection is critical to the innovation cycle for business of all sizes across industry sectors. Unfortunately, the information and know-how protected as trade secrets are particularly vulnerable to misappropriation. Companies that operate globally experience trade secret theft domestically, they experience it overseas, and they experience it domestically for purposes of using it overseas.

Wherever trade secret theft happens, it harms innovation and job creation, and we therefore appreciate Congress's attention to this matter.

Question 2. Do you support legislation that would provide additional tools to protect companies against domestic and foreign trade secret theft?

Answer: Eli Lilly and Company and the Protect Trade Secrets Coalition support a uniform, harmonized system for protecting trade secrets both domestically and abroad. The tools thieves are using in their attempts to steal our trade secrets are growing more sophisticated and our laws need to keep pace.

We support the Defend Trade Secrets Act because it will provide a uniform federal remedy for trade secret owners that will enhance our ability to act quickly and effectively when our trade secrets are stolen. This would put trade secret protection in-line with the remedies available to owners of other forms intellectual property.

In addition, the legislation would establish the gold standard for trade secret laws globally, which is important in our effort to prevent foreign trade secret theft. We appreciate your focus on the foreign component of the problem, and we look forward to working with you on our shared objective of protecting trade secrets and thereby encouraging investment in research, innovation, and job creation.

Responses of Pamela Passman to Questions Submitted by Senator Flake

Hearing on "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?"

Questions for the Record from Senator Flake for Pamela Passman

Question 1. Do you agree that both domestic and foreign misappropriation of trade secrets is a growing and persistent problem?

Answer: Yes. Companies are increasingly relying on trade secret laws to protect their investment in research and development. Our experience at CREATe has made it apparent that trade secrets are critical to a company's innovation and competitiveness.

The tremendous value of trade secrets also makes them targets for theft. Trade secret theft occurs through many vectors, including cybercrime, disgruntled employees, malicious insiders, competitors, nation-states, hactivists, and transnational criminal organizations. The growth of global supply chains, through which companies often must share confidential and highly valuable business information with suppliers, increases the risk of both domestic and foreign trade secret theft.

Question 2. Do you support legislation that would provide additional tools to protect companies against domestic and foreign trade secret theft?

Answer: CREATe does not take formal positions on legislation. We do think it is important, however, for there to be a predictable, harmonized legal system both domestically and abroad to provide effective remedies when a trade secret theft occurs. The Defend Trade Secrets Act is geared toward providing a predictable and harmonized system in the United States, which would benefit companies doing business here; it can also serve as a model for our trading partners, which would benefit companies that rely on a global supply chain and have their trade secrets at risk around the world.