

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

78-99 minutes

[Senate Hearing 113-780]
[From the U.S. Government Publishing Office]

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

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

U.S. GOVERNMENT PUBLISHING OFFICE

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 GRASSLEY, Iowa, Ranking
CHUCK SCHUMER, New York Member
DICK DURBIN, Illinois ORRIN G. HATCH, Utah
SHELDON WHITEHOUSE, Rhode Island JEFF SESSIONS, Alabama
AMY KLOBUCHAR, Minnesota LINDSEY GRAHAM, South Carolina
AL FRANKEN, Minnesota JOHN CORNYN, Texas
CHRISTOPHER A. COONS, Delaware MICHAEL S. LEE, Utah
RICHARD BLUMENTHAL, Connecticut TED CRUZ, Texas
MAZIE HIRONO, Hawaii 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 LINDSEY GRAHAM, South Carolina,
CHUCK SCHUMER, New York Ranking Member
DICK DURBIN, Illinois TED CRUZ, Texas
AMY KLOBUCHAR, Minnesota JEFF SESSIONS, Alabama
MICHAEL S. LEE, Utah
Ayo Griffin, Democratic Chief Counsel
David Glaccum, Republican Chief Counsel

C O N T E N T S

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 appointment 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, consumer 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 implement 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 co-founder 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 engineers. 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 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.]

A P P E N D I X

Additional Material Submitted for the Record

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Prepared Statement of Chairman Patrick Leahy

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Prepared Statement of Chairman Sheldon Whitehouse

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Prepared Statement of Randall C. Coleman

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Prepared Statement of Peter L. Hoffman

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Prepared Statement of Pamela Passman

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Prepared Statement of Drew Greenblatt

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Prepared Statement of Douglas K. Norman

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Questions Submitted to Randall C. Coleman
by Senator Whitehouse

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Questions Submitted to Peter L. Hoffman by Senator Flake

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Questions Submitted to Douglas K. Norman
by Senator Flake

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Questions Submitted to Pamela Passman by Senator Flake

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Responses of Randall C. Coleman to Questions Submitted
by Senator Whitehouse

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Responses of Peter L. Hoffman to Questions Submitted
by Senator Flake

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Responses of Douglas K. Norman to Questions Submitted
by Senator Flake

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

Responses of Pamela Passman to Questions Submitted
by Senator Flake

[GRAPHIC(S) NOT AVAILABLE IN TIFF FORMAT]

[all]