ECONOMIC ESPIONAGE: A FOREIGN INTELLIGENCE THREAT TO AMERICAN JOBS AND HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JUNE 28, 2012

Serial No. 112–101

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

79–843 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
RON BARBER, Arizona

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PATRICK MEEHAN, Pennsylvania, *Chairman*

PAUL C. BROUN, Georgia, *Vice Chair*
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
PETER T. KING, New York *(Ex Officio)*

BRIAN HIGGINS, New York
LORETTA SANCHEZ, California
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
RON BARBER, Arizona
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

KEVIN GUNDERSEN, *Staff Director*
ZACHARY HARRIS, *Subcommittee Clerk*
HOPE GOINS, *Minority Subcommittee Director*

CONTENTS

Page

STATEMENTS

The Honorable Billy Long, a Representative in Congress From the State of Missouri:
Oral Statement 1
Prepared Statement 3
The Honorable Brian Higgins, a Representative in Congress From the State of New York, and Ranking Member, Subcommittee on Counterterrorism and Intelligence 5

WITNESSES

Mr. Stuart Graham, Chief Economist, U.S. Patent and Trademark Office, U.S. Department of Commerce:
Oral Statement 8
Prepared Statement 9
Mr. John P. Woods, Assistant Director, Homeland Security Investigations, Immigration and Customs Enforcement, U.S. Department of Homeland Security:
Oral Statement 12
Prepared Statement 14
Mr. C. Frank Figliuzzi, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, U.S. Department of Justice:
Oral Statement 16
Prepared Statement 18
Mr. Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office:
Oral Statement 19
Prepared Statement 21

ECONOMIC ESPIONAGE: A FOREIGN INTELLIGENCE THREAT TO AMERICAN JOBS AND HOMELAND SECURITY

Thursday, June 28, 2012

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:05 a.m., in Room 311, Cannon House Office Building, Hon. Billy Long presiding.

Present: Representatives Long, Higgins, and Hochul.

Mr. LONG. The Committee on Homeland Subcommittee on Counterterrorism and Intelligence will come to order.

The subcommittee is meeting today to hear testimony regarding economic espionage and its threat to American jobs and homeland security. As most of you know, Chairman Meehan is not at today's hearing. Unfortunately, an issue arose that he had to attend, and I will be chairing today's hearing.

I recognize myself for an opening statement. The National unemployment rate currently stands at 8.2 percent, and our Nation faces economic headwinds. Over the last 2 years, we have examined many threats to the U.S. homeland. However, today's hearing provides an opportunity, a unique opportunity, for Members on the subcommittee to examine an issue that affects both National security and American competitiveness and job security.

This is an issue that touches small and medium-sized businesses in Congressional districts all across America. Foreign economic and industrial espionage against the United States represents a significant and growing threat to the Nation's prosperity, American jobs, and National security. The primary strengths of the private sector in the United States are its tangible assets, including research and development, intellectual property, sophisticated business processes, and enforceable contracts.

Unfortunately, those assets are being stolen by foreign intelligence services, corporations with close ties to foreign governments, and non-state actors. According to the U.S. Army General Keith Alexander, director of the National Security Agency and commander of U.S. Cyber Command, the United States currently finds itself the victim of the greatest transfer of wealth in history.

Just this week, the director of the British's international security agency, MI5, told a London audience that it is investigating cyber attacks against more than a dozen companies, and added that one major London business has suffered more than $1.2 billion in

losses from an attack. He called the extent of the espionage activity astonishing, with industrial-scale process, involving many thousands of people lying behind both state-sponsored cyber espionage and organized crime.

This spring, FBI erected billboards at nine cities around the country to highlight the $13 billion in losses suffered by U.S. companies as a result of economic espionage in 2012 alone. While that number is staggering, my fear is that the $13 billion represents only the tip of the iceberg. Of even greater concern is finding out what lies beneath the surface.

Due to a number of factors, which will be discussed today, the true size of this threat could be massively undervalued because this activity often goes unreported to law enforcement. Economic espionage can take many forms, including visits to a company's website to gather open-source information, and employees downloading proprietary information on a thumb drive at the behest of a foreign rival. Or intrusions launched by foreign intelligence service or other actors against the company's network of a private company, Federal agency, or individual.

Unlike 20 years ago, business activity conducted over the internet provides opportunities for bad actors to infiltrate and steal vital data from the U.S. companies. Cyberspace also provides relatively small-scale actors an environment and opportunity to become big players in economic espionage.

In addition, under-resourced governments or corporations often build relationships with hackers to steal sensitive economic or technological information just as national states have done for decades. In many ways, the threat posed by the economic espionage is similar to the threat posed by al-Qaeda and its affiliate networks, less centralized and more diffuse. And making it, often, more difficult to combat.

Making this an even more complex problem, many bad actors often remain anonymous, and determining attribution of attacks is difficult for law enforcement in the intelligence community. Many actors route operations through computers in third countries, or physically operate from third-party countries to obscure the origins of a activity.

Some foreign intelligence services and non-state actors have reportedly used independent hackers at times to augment their capabilities and act as proxies for intrusions in order to provide plausible deniability. Both China and Russia view economic espionage as an essential tool in statecraft to achieve stated National security and economic prosperity aims.

It is critical Members of Congress and U.S. businesses understand that point; China and Russia have official government policies of stealing U.S. assets for economic gain. They target sensitive U.S. technology and economic data, private-sector companies, academic and research institutions, and U.S. citizens on a daily basis.

According to the National Counterintelligence Executive, China and Russia will remain aggressive collectors of sensitive U.S. economic information and technology. Both countries will certainly continue to deploy significant resources and a wide variety of tactics to acquire this information, motivated by the desire to achieve economic, strategic, and military parity with the United States.

Unfortunately, many private-sector victims of economic espionage are unaware of the crime until years after the loss of their information. In addition, many companies that are victims of espionage choose not to report the event to the FBI because it would negatively affect the company's reputation and endanger its relationship with investors, bankers, suppliers, customers, and shareholders.

In many cases, it is difficult for companies to assign an economic value to stolen information, thereby decreasing their incentive to share information with law enforcement. A few examples I would like to point out that illustrate the challenge faced by the private sector. The AMSC Corporation, a Massachusetts-based maker of computer systems that run wind turbines, was victimized by its largest customer, China's C-Nobel Corporation.

C-Nobel illegally obtained access to AMSC's proprietary source code through an AMSC employee who was paid to aid in the theft. C-Nobel, which accounted for two-thirds of AMSC's annual revenue of $315 million took AMSC's source code, began producing its own computers, and severed its relationship with AMSC.

When this news was made public, AMSC's share price fell 40 percent in a single day. Over the course of 5 months it plunged 84 percent. One U.S. metals company lost technology to China's hackers that cost $1 billion and 20 years to develop. An employee of the Valspar Corporation unlawfully downloaded proprietary paint formulas valued at $20 million which he intended to take to a new job in China, according to press reports.

This theft represented about one-eighth of Valspar's reported profits for 2009, the year the employee was arrested. Today's witness—let us see—to get to a better understanding of the problem, today we will hear from a panel of Government witnesses from the FBI, Immigration and Customs Enforcement, and the Department of Commerce about the nature and severity of the threat and its cost to the U.S. economy.

We will also learn what the U.S. Government is doing to combat the threat, including its work with small and medium-sized businesses to prevent the loss of trade secrets and intellectual property. I look forward to hearing from today's witnesses on this important topic.

[The statement of Hon. Long follows:]

STATEMENT OF HON. BILLY LONG

JUNE 28, 2012

NATIONAL SECURITY AND JOB SECURITY

The National unemployment rate currently stands at 8.2% and our Nation faces tough economic headwinds. Over the last 2 years, we have examined many threats to the U.S. homeland.

However, today's hearing provides a unique opportunity for Members of the subcommittee to examine an issue that affects both National security and American competitiveness and job security. This is an issue that touches small and medium-sized businesses in Congressional districts all across America.

ECONOMIC ESPIONAGE THREAT

Foreign economic and industrial espionage against the United States represents a significant and growing threat to the Nation's prosperity, American jobs, and National security. The primary strengths of the private sector in the United States are

its tangible assets, including research and development (R&D), intellectual property, sophisticated business processes, and enforceable contracts.

Unfortunately, those assets are being stolen by foreign intelligence services, corporations with close ties to foreign governments, and non-state actors. According to U.S. Army General Keith Alexander, Director of the National Security Agency and Commander of U.S. Cyber Command, the U.S. currently finds itself the victim of "the greatest transfer of wealth in history."

Just this week, the Director General of Britain's internal security agency, MI5 told a London audience that it is investigating cyber attacks against more than a dozen companies and added that one major London business had suffered more than $1.2 billion dollars in losses from an attack. He called the extent of the espionage activity "astonishing—with industrial-scale processes involving many thousands of people lying behind both state-sponsored cyber-espionage and organized crime."

This spring FBI erected billboards in nine cities around the country to highlight the $13 billion dollars in losses suffered by U.S. companies as a result of economic espionage in 2012 alone. While that number is staggering, my fear is that the $13 billion represents only the tip of the iceberg. Of even greater concern is finding out what lies beneath the surface. Due to a number of factors, which will be discussed today, the true size of this threat could be massively under-valued because this activity often goes unreported to law enforcement.

EVOLVING THREAT ENVIRONMENT & CYBER THREAT

Economic espionage can take many forms including, visits to a company's website to gather open-source information; an employee's downloading of proprietary information onto a thumb drive at the behest of a foreign rival; or intrusions launched by a foreign intelligence service or other actors against the computer networks of a private company, Federal agency, or an individual.

Unlike 20 years ago, business activity conducted over the internet provides opportunities for bad actors to infiltrate and steal vital data from U.S. companies. Cyberspace also provides relatively small-scale actors an environment and opportunity to become big players in economic espionage.

In addition, under-resourced governments or corporations often build relationships with hackers to steal sensitive economic or technological information, just as national states have done for decades.

In many ways, the threat posed by economic espionage is similar to the threat posed by al-Qaeda and its affiliate networks: Less centralized and more diffuse, often making if more difficult to combat.

ANONYMITY AND ATTRIBUTION

Making this an even more complex problem, many bad actors often remain anonymous and determining attribution of attacks is difficult for law enforcement and the intelligence community.

Many actors route operations through computers in third countries or physically operate from third-party countries to obscure the origin of their activity. Some foreign intelligence services and non-state actors have reportedly used independent hackers at times to augment their capabilities and act as proxies for intrusions in order to provide plausible deniability.

CHINA AND RUSSIA

Both China and Russia view economic espionage as an essential tool in statecraft to achieve stated National security and economic prosperity aims. It is critical Members of Congress and U.S. businesses understand that point: China and Russia have official government policies of stealing U.S. assets for their economic gain.

They target sensitive U.S. technology and economic data, private-sector companies, academic and research institutions, and U.S. citizens on a daily basis. According to the National Counterintelligence Executive, China and Russia will remain aggressive collectors of sensitive U.S. economic information and technology. Both countries will certainly continue to deploy significant resources and a wide array of tactics to acquire this information, motivated by the desire to achieve economic, strategic, and military parity with the United States.

PRIVATE-SECTOR CHALLENGES

Unfortunately, many private-sector victims of economic espionage are unaware of the crime until years after the loss of their information. In addition, many companies that are victims of espionage choose not to report the event to the FBI because

it would negatively affect the company's reputation and endanger its relationships with investors, bankers, suppliers, customers, and shareholders.

In many cases, it is difficult for companies to assign an economic value to stolen information, thereby decreasing their incentive to share information with law enforcement.

EXAMPLES OF ESPIONAGE

A few examples I'd like to point out that illustrate the challenge faced by the private sector:

- The AMSC Corporation, a Massachusetts-based maker of computer systems that run wind turbines, was victimized by its largest customer, China's Sinovel Corporation. Sinovel illegally obtained access to AMSC's proprietary source code through an AMSC employee, who was paid to aid in the theft. Sinovel, which accounted for two-thirds of AMSC's annual revenue of $315 million, took AMSC's source code, began producing its own computers and severed its relationship with AMSC. When this news was made public AMSC's share price fell 40% in a single day and over the course of 5 months plunged 84%.
- One U.S. metallurgical company lost technology to China's hackers that cost $1 billion and 20 years to develop.
- An employee of the Valspar Corporation unlawfully downloaded proprietary paint formulas valued at $20 million, which he intended to take to a new job in China, according to press reports. This theft represented about one-eighth of Valspar's reported profits in 2009, the year the employee was arrested.

TODAY'S WITNESSES

To get a better understanding of this problem, today we will hear from a panel of Government witnesses from the FBI, Immigration and Customs Enforcement (ICE), and the Department of Commerce about the nature and severity of the threat and its costs to the U.S. economy. We will also learn what the U.S. Government is doing to combat the threat, including its work with small and medium-sized businesses to prevent the loss of trade secrets and intellectual property.

I look forward to hearing from today's witnesses on this important topic.

Mr. LONG. The Chairman now recognizes the Ranking Member of the Subcommittee on Counterterrorism and Intelligence, the gentleman from New York, Mr. Higgins, for any statement he may have.

Mr. HIGGINS. Thank you, Mr. Chairman. I would also like to thank you for holding this important hearing.

Tom Friedman, in his book The World is Flat, discusses today's global web-enabled world that allows everybody to plug in and play, sharing knowledge, work irrespective of time, distance, geography and, increasingly, language. This paradigm makes the United States a target for economic espionage, where other nations work covertly to obtain sensitive technology and economic information to undermine our status as a global economic leader.

Economic espionage is not a new concept. It has posed a threat to the United States' National security for decades. But now it has become an issue for American businesses, as well. According to the FBI, the United States' companies suffered more than $13 billion in economic losses in fiscal year 2012 alone.

This is an appalling figure. What is more astonishing is that we cannot value the true long-term cost of theft in transfer of intellectual property. But we know it is significant. Economic espionage, through cyber attacks committed by foreign intelligence services and other criminal enterprises is so pervasive that in a recent poll 90 percent—90 percent—of companies admitted their networks had been breached in the past 12 months; while the other 10 percent could not say with certainty that they had not been penetrated.

According to the former White House cybersecurity advisor, Richard Clarke, every major company in the United States has already been penetrated by China. The Chinese have been linked to a wide range of economic espionage in recent years, including the theft of blueprints for the next-generation stealth fighter from a defense contractor.

Last month, in a report issued by the Pentagon, officials stated that China would continue to be an aggressive and capable collector of sensitive U.S. technological information. Additionally, in its report to Congress, the Office of National Counterintelligence Executive judged that the most active and persistent perpetrator of economic espionage is China.

China is not the only country focused on the United States. Russia is also identified as aggressive in their pursuit of U.S. trade secrets. Further, just about 2 months ago this subcommittee also heard from witnesses that stated that our critical infrastructure was vulnerable to attack from Iran. Given the wealth of trade secrets in America, I am sure it would be possible for it to be vulnerable to espionage from other countries aside from those who have been mentioned.

Knowing these facts, the administration is right to take steps to address economic espionage, and I am looking forward to learning more from the testimony today. I hope that they can give us as much insight as they can in an open setting. Although the administration has issued these stern warnings of the threat of economic espionage in reports and through advertisements, Congress has not responded adequately.

Key legislation that would have helped protect our most sensitive industries and critical infrastructure from cyber intrusions were not even allowed to be considered by the House. We were disappointed by the Majority's philosophy with respect to these issues, and we are hoping that this testimony will help pave the way for greater transparency and more decisive action.

Right now, our cybersecurity legislation is lacking with respect to critical infrastructure. But it seems as if right now is—the Government and companies will deal with resources that are currently available. I look forward to learning how the agencies are dealing with this issue, and if they are cooperating with each other to prevent the devastation of economic espionage.

With that, I will yield back.

Mr. LONG. Thank you, Ranking Member Higgins.

Other Members of the committee are reminded that opening statements may be submitted for the record. We are pleased to have a distinguished panel of witnesses before us today on this important topic.

Dr. Stuart Graham is the chief economist at the U.S. Patent and Trademark Office, where he manages a team of economists researching the impact of intellectual property on the economy. Dr. Graham's research focuses on the economics of the patent system, intellectual property transactions, and relationships of intellectual property to entrepreneurship, and to commercialization of new technologies.

Dr. Graham has testified about the patent system before the U.S. Federal Trade Commission, and has served as a scientific expert to

the European patent office, the European trademark office, Industry Canada, and the Organization of Economic Cooperation and Development. He is currently serving as the chief economist while on leave from his academic post at Georgia Tech. Welcome.

Mr. John Woods currently serves as the assistant director of the National Security Investigations Division, which is part of the U.S. Immigration and Customs Enforcement Homeland Security's Investigations. Mr. Woods has served in this position since April 2009, overseeing 450 people and managing a $160 million operational budget.

Mr. Woods has 26 years of experience in law enforcement, the majority of that time developing and managing programs for the U.S. Immigration and Naturalization Service and HSI. Previously, Mr. Woods served as a deputy assistant director of the National Security Investigations Division, the unit chief of ICE's counterterrorism unit, and the assistant special agent in charge of the Miami SAC office.

During this career with INS, he served as a section chief for the Miami district office, and has also served as a supervisory agent in Washington, DC and New York City. Mr. Woods began his Federal law enforcement career in New York City as an INS agent back in 1987. Welcome, Mr. Woods.

Mr. Frank Figliuzzi is the assistant director of the FBI's counterintelligence division. Mr. Figliuzzi has been the division's deputy assistant director since November 2010. He was appointed as an FBI special agent in August 1987 and assigned to the Atlanta division, working on terrorism and foreign counterintelligence investigations

He was promoted to the National Security Division at the FBI's headquarters in Washington, DC, with the responsibility of oversight of economic espionage matters. Prior to his appointment as deputy assistant director, Mr. Figliuzzi served as the FBI's chief inspector, the chief unit of the Office of Professional Responsibility, at FBI headquarters, and supervisory senior resident agent for the FBI's San Francisco division. Welcome, Mr. Figliuzzi.

Mr. Greg Wilshusen is the director of information security issues at the Government Accountability Office, GAO, where he leads information, security-related studies, and audits of the Federal Government. He has over 28 years of auditing, financial management, and information systems experience.

Prior to joining GAO in 1997, Mr. Wilshusen held a variety of public and private-sector positions. He was a senior systems analyst at the Department of Education. He also served as the controller for the North Carolina Department of Environment, Health, and Natural Resources, and held several auditing positions at Irving Burton Institutes, Incorporated and the United States Army Audit Agency. Welcome, Mr. Wilshusen. Just hope I am saying that right.

The Chairman now recognizes Dr. Graham to testify.

STATEMENT OF STUART GRAHAM, CHIEF ECONOMIST, U.S. PATENT AND TRADEMARK OFFICE, U.S. DEPARTMENT OF COMMERCE

Mr. GRAHAM. Chairman Long, Ranking Member Higgins, and Members of the subcommittee. Thank you for giving me the opportunity today to testify on the importance of intellectual property protections to the American economy.

I am currently serving in the United States Patent and Trademark Office, or under Secretary David Kappos, as the first chief economist in the agency's history. While serving, I am on leave from my academic position at Georgia Tech's Sheller College of Business.

My testimony today will focus primarily on the potential impact of economic espionage on one of this country's most important resources; the valuable, intangible assets held by American innovators and safeguarded by intellectual property protections both here and abroad. In a real sense, we cannot appreciate the scope of the potential espionage problem unless we recognize how important IP protections are to U.S. businesses and industries.

Mr. Chairman, on April 11, 2012 the Department of Commerce released a report titled Intellectual Property in the U.S. Economy: Industries in Focus. This report details how U.S. companies in our most competitive industries are using patents, copyright, and trade secrets to protect their innovations, and trademarks to distinguish their goods and services from those of competitors.

These protections are important supports for the American innovation system, enabling companies to capture market share and effectively sell and export goods, in turn contributing to economic growth and to America's overall competitiveness. The report identifies the 75 American industries most intensively using IP protections, and uses statistical data from across the U.S. Government to examine both the important trends and economic characteristics of these highly IP-intensive industries.

There are several important findings contained in the report, including the following. First, the entire U.S. economy relies on some form of IP because virtually every industry either produces it or uses it. During 2010, the IP-intensive industries directly accounted for about 27 million American jobs, and indirectly supported an additional 13 million jobs in the supply chain.

This totals 40 million American jobs, or just under 28 percent of all U.S. employment. Jobs in the IP-intensive industries pay well compared to other jobs. In 2010, average weekly wages for these industries were 42 percent higher than wages elsewhere in the economy. That pay differential was an impressive 70 percent higher for jobs in the patent- and copyright-intensive industries.

Moreover, the IP-intensive industries accounted for just over $5 trillion in value added in 2010, or about 35 percent of the United States gross domestic product. Finally, merchandise exports of IP-intensive industries totaled $775 billion in 2010. That accounted for just under 61 percent of total U.S. merchandise exports.

Mr. Chairman, in light of increasing concerns about IP infringement and misappropriation, the Department of Commerce is emphasizing this area in our domestic and foreign policy objectives. At the USPTO, for instance, we are providing American businesses

with information and training such as our China IP toolkit, available to the public on the website stopfakes.gov.

The USPTO is also especially proud of our IP attachés program. Currently, we have representatives on the ground in each of the BRIC countries, with 2 attachés currently serving in China helping U.S. companies to navigate through the IP challenges they face there.

It is important to note that there are many efforts underway across the Department of Commerce, ranging from the Bureau of Industry and Securities Enforcement activities and administrative sanctions against export violators to outreach and advocacy across the Department directed at helping U.S. companies compete successfully in foreign markets.

In conclusion, Mr. Chairman, the growth, job creation, and success of businesses of all shapes and sizes in the U.S. economy are dependent on the effectiveness of IP protection. The Department of Commerce is committed to supporting American innovation, including the ability of U.S. businesses to compete fairly and by protecting our economy from illegal copying and theft.

We appreciate your support for the employees and operations of the Department that make that protection possible. Thank you.

[The statement of Mr. Graham follows:]

PREPARED STATEMENT OF STUART GRAHAM

JUNE 28, 2012

INTRODUCTION

Chairman Meehan, Ranking Member Higgins, and Members of the subcommittee: Thank you for this opportunity to discuss the potential impact of economic espionage on one of this country's most important resources—the intellectual property (IP) protections of our innovators.

It is clear that policies supporting and protecting a higher-quality IP system are making a difference in our Nation's economic recovery. In my testimony today, I will primarily discuss the importance of IP protections to U.S. businesses, with particular focus on the findings contained in the Department of Commerce's recent report titled "Intellectual Property in the U.S. Economy: Industries in Focus." Moreover, I will discuss actions the Department of Commerce is taking to build capacity in the United States for new and existing businesses to protect their innovations. The Department of Commerce is keenly aware that America's core strength lies in our ability to experiment, innovate, and create new value. It is axiomatic that sensible Government policies that encourage and stimulate that spirit of innovation and clear that appropriate protection for American innovation can demonstrably contribute to job creation, economic well-being, and better lives for our people.

COMMERCE REPORT OVERVIEW: "INTELLECTUAL PROPERTY IN THE U.S. ECONOMY: INDUSTRIES IN FOCUS"

On April 11, 2012, the Department of Commerce released this report in a White House press conference. Underlining the importance of this topic, speakers included the Secretary of Commerce, the White House Intellectual Property Coordinator, the President of the U.S. Chamber of Commerce, and the President of the AFL–CIO. The report is a collaborative effort by economists in the Economics and Statistical Administration (ESA) and the United States Patent and Trademark Office (USPTO), both bureaus of the Department. This report has had a large impact in helping to educate citizens about the role of intellectual property in our economic health—during the first 30 days after the report's release it was downloaded from the USPTO website over 82,000 times.

The report recognizes that innovation—the process through which new ideas are generated and successfully introduced in the marketplace—is a primary driver of

U.S. economic growth and National competitiveness.[1] U.S. companies' use of patents, copyright, and trade secrecy to protect their creations, and trademarks to distinguish their goods and services from those of competitors represent important supports for innovation, enabling firms to capture market share, which contributes to growth in our economy. The granting and protection of intellectual property rights is vital to promoting innovation and creativity and is an essential element of our free enterprise, market-based system. Patents, trademarks, and copyrights are the principal means used to establish ownership of inventions and creative ideas in their various forms, providing a legal foundation to generate tangible benefits from innovation for companies, workers, and consumers. Without this framework, the creators of intellectual property would tend to lose the economic fruits of their own work, thereby undermining the incentives to undertake the investments necessary to develop the IP in the first place.[2] Moreover, without IP protection, the inventor who had invested time and money in developing the new product or service (sunk costs) would always be at a disadvantage to the new firm that could just copy and market the product without having to recoup any sunk costs or pay the higher salaries required by those with the creative talents and skills. As a result, the benefits associated with American ingenuity would tend to more easily flow outside the United States.

The report finds that IP is used everywhere in the economy, and IP rights support innovation and creativity in virtually every U.S. industry. While IP rights play a large role in generating economic growth, too little attention has been given to identifying which industries produce or use significant amounts of IP and rely most intensively on these rights. The report was written to give policy makers and the public more information about the impacts of IP protection in the U.S. economy on which to base sound policy.

This report investigates the economic impact in the United States of intellectual property protection by developing several industry-level metrics on IP use and employs these measures to identify a set of the most IP-intensive industries in the U.S. economy. To develop the industry-level metrics discussed, several databases were used, some of which (for the patent and trademark analyses) are publicly available.[3]

The report employs USPTO administrative data to identify the industries that most intensively use the protection offered by patents and trademarks. For copyrights, the report identifies the set of industries primarily responsible for both the creation and production of copyrighted materials. The report then uses standard statistical methods to identify which American industries are the most patent-, trademark-, and copyright-intensive, and defines this subset of industries as "IP-intensive." Using data collected from sources across the U.S. Government, the report examines both the important trends and economic characteristics of these highly IP-intensive industries, and their meaningful contributions to the U.S. economy. There are several important findings contained in the report.

COMMERCE REPORT FINDINGS

Mr. Chairman, the important findings of the Department's report are as follows:

- The entire U.S. economy relies on some form of IP, because virtually every industry either produces or uses it.
- IP-intensive industries accounted for about $5.06 trillion in value added, or 34.8% of U.S. gross domestic product (GDP), in 2010. Merchandise exports of IP-intensive industries totaled $775 billion in 2010, accounting for 60.7% of total U.S. merchandise exports.
- IP-intensive industries directly accounted for 27.1 million American jobs, or 18.8% of all employment in the economy, in 2010.
- A substantial share of IP-intensive employment in the United States was in the 60 trademark-intensive industries, with 22.6 million jobs in 2010. The 26 patent-intensive industries accounted for 3.9 million jobs in 2010, while the 13 copyright-intensive industries provided 5.1 million jobs.
- While IP-intensive industries directly supported 27.1 million jobs either on their payrolls or under employment contracts, these sectors also indirectly supported 12.9 million more supply chain jobs throughout the economy.
- In other words, every two jobs in IP-intensive industries support an additional one job elsewhere in the economy. In total, 40.0 million jobs, or 27.7% of all jobs, were directly or indirectly attributable to the most IP-intensive industries.

---

[1] National Economic Council et al. 2011.

[2] Ibid., 11.

[3] See *www.uspto.gov/web/offices/ac/ido/oeip/taf/data/naics_conc/* and also *www.google.com/googlebooks/usptotrademarks.html.*

- Jobs in IP-intensive industries pay well compared to other jobs. Average weekly wages for IP-intensive industries were $1,156 in 2010 or 42% higher than the $815 average weekly wages in other (non-IP-intensive) private industries. This wage premium nearly doubled from 22% in 1990 to 42% by 2010.
- Patent- and copyright-intensive industries have seen particularly fast wage growth in recent years, with the wage premium in patent-intensive industries increasing from 66% in 2005 to 73% in 2010. And the premium in copyright-intensive industries rising from 65% to 77%.
- The comparatively high wages in IP-intensive industries correspond to, on average, the completion of more years of schooling by these workers. More than 42% of workers aged 25 and over in these industries in 2010 were college-educated, compared with 34% on average in non-IP intensive industries.
- Due primarily to historic losses in manufacturing jobs, overall employment in IP-intensive industries has lagged other industries during the last 2 decades. While employment in non-IP intensive industries was 21.7% higher in 2011 than in 1990, overall IP-intensive industry employment grew 2.3% over this same period.
- Because patent-intensive industries are all in the manufacturing sector, they experienced relatively more employment losses over this period, especially during the past decade.
- While trademark-intensive industry employment had edged down 2.3% by the end of this period, copyright-intensive industries provided a sizeable employment boost, growing by 46.3% between 1990 and 2011.
- Between 2010 and 2011, the economic recovery led to a 1.6% increase in direct employment in IP-intensive industries, faster than the 1.0% growth in non-IP-intensive industries.
- Growth in copyright-intensive industries (2.4%), patent-intensive industries (2.3%), and trademark-intensive industries (1.1%) all outpaced gains in non-IP-intensive industries.
- Data on foreign trade of IP-intensive service-providing industries is limited. However, this report does find that exports of IP-intensive service-providing industries accounted for approximately 19% of total U.S. private services exports in 2007.

THE IMPORTANCE OF PROTECTIONS TO U.S. BUSINESSES

Mr. Chairman, it is important to point out that the findings contained in the Commerce report concerning the positive economic impacts of the most intensive users of IP in the economy are consistent with previous academic studies finding that secrecy, patenting, and other legal protections are important to U.S. businesses in securing competitive advantage from their innovations. Notably, in response to a survey conducted by scholars at Carnegie-Mellon University in the 1990s, managers of U.S. businesses reported that various legal protections were effective in protecting their product and process innovations. Across all industries surveyed, patenting was found to effectively protect U.S. business' competitive advantage for over one-third of their product innovations, while secrecy was found to effectively protect competitive advantage on innovations in over one-half of product and process innovations.[4]

Given recent evidence from the Kauffman Foundation showing that new business creation disproportionately contributes to job creation in the United States,[5] it is important to note that a recent survey conducted at the University of California examining only young companies in high-technology industries finds results similar to the Carnegie-Mellon survey.[6] Managers at start-up companies told the researchers in 2008 that patents, trademarks, copyright, and trade secret protections were all important to securing competitive advantage from their new product and process innovations. Notably, the most important reason that managers cited for seeking patent protection was to prevent others from copying their products or services.

---

[4] Cohen, Wesley M., Richard R. Nelson, and John P. Walsh (2000). "Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)." NBER Working Paper 7552, available at *http://www.nber.org/papers/w7552.*

[5] See, e.g., Tim J. Kane (2010). "The Importance of Startups in Job Creation and Job Destruction," SSRN working paper, available at *http://ssrn.com/abstract=1646934;* E.J. Reedy & Robert E. Litan (2011). "Starting Smaller; Staying Smaller: America's Slow Leak in Job Creation," SSRN working paper, available at *http://ssrn.com/abstract=1883660.*

[6] Graham, Stuart, Robert P. Merges, Pamela Samuelson, and Ted M. Sichelman (2009). "High Technology Entrepreneurs and the Patent System: Results of the 2008 Berkeley Patent Survey. Berkeley Technology Law Journal, Vol. 24, No. 4, pp. 255–327, available at *http://ssrn.com/abstract=1429049.*

DEPARTMENT OF COMMERCE EFFORTS TO BUILD CAPACITY AND PROTECT AMERICAN INNOVATION

In light of the recent and increasing concerns by U.S. right holders on the importance of having effective mechanisms to protect their trade secrets from misappropriation, the USPTO is emphasizing this area in our domestic and foreign policy objectives, particularly as they relate to other countries. USPTO attorneys are undertaking a comprehensive study of foreign laws and other legal measures governing trade secrets and are discussing with foreign government officials changes that can facilitate more effective protection regimes abroad. For instance, USPTO is using this information to update the "China IP Toolkit" on Stopfakes.gov with a section dedicated to trade secret protection and enforcement. This component of the Toolkit will provide an overview of China's major laws and other measures affecting trade secrets and include basic steps a company can consider to protect its trade secrets in China, including not only information on judicial and administrative enforcement mechanisms but also basic strategies companies can employ to help prevent misappropriation from occurring.

Also, the USPTO is currently developing training modules on trade secrets for small and medium enterprises and enforcement officials. These modules will include an overview of trade secret law in the United States, measures to protect trade secrets, criminal and civil enforcement procedures, and international trade secret protection and enforcement.

My presentation today focuses on USPTO efforts in support of the administration's innovation goals. I would like to note, however, that there are additional efforts underway across the Department of Commerce, ranging from BIS's enforcement activities and administrative sanctions against export violators, to outreach and advocacy directed at helping U.S. IP-intensive industries compete successfully in foreign markets.

CONCLUSION

Mr. Chairman, the growth, job creation, and success of businesses of all shapes and sizes are highly dependent on the effectiveness of IP protection. The Department of Commerce is committed to supporting not only the creation of innovation, but also the ability of U.S. businesses to compete fairly with these innovations and protect our economy from illegal copying and theft. We appreciate your support for the employees and operations of the Department that make that protection possible.

Mr. LONG. Thank you, Dr. Graham.

The Chairman now recognizes Mr. Woods to testify.

STATEMENT OF JOHN P. WOODS, ASSISTANT DIRECTOR, HOMELAND SECURITY INVESTIGATIONS, IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. WOODS. Chairman Long, Ranking Member Higgins, and distinguished Members of the subcommittee, I thank you for the opportunity to discuss ICE's efforts to combat intellectual property and technology fraud by foreign governments. The theft of U.S. proprietary technology, including controlled dual-use technology and military-grade equipment, from unwitting U.S. companies is one of the most dangerous threats to our National security.

By maintaining investigative partnerships with other law enforcement agencies both in the United States and internationally, ICE is at the forefront of our Nation's efforts to investigate these threats. ICE's Homeland Security Investigations handles a wide range of trade fraud investigations, including IP theft, commercial fraud, and export violations.

I would like to begin my discussion with our counter-proliferation investigations program, which targets the trafficking and/or illegal export of conventional military equipment, firearms, controlled dual-use equipment and technology, and materials used to manu-

facture weapons of mass destruction, including chemical, biological, radiological, and nuclear materials.

HSI's special agents investigate illegal exports of military equipment and dual-use technologies to embargo countries, and significant financial and business transactions with these proscribed countries and/or groups. We also conduct export enforcement training with foreign law enforcement agencies, and provide outreach with private industries in the United States and internationally.

HSI's export enforcement program uses a three-pronged approach. Detecting the illegal exports, investigating those potential violations, and obtaining international cooperation to investigate leads abroad. One of the most effective tools that we use is our industry outreach program, called Project Shield America. Through this program, we conduct outreach to manufacturers, exporters of strategic commodities to educate them on the U.S. export control laws, discuss export licensing issues and requirements, and identify the red-flag indicators used in illicit procurement.

To date, we have delivered over 20,000 outreach presentations to private industry and other entities as part of the program. As part of the President's export control reform initiative, it is to improve law enforcement coordination to investigate violations of U.S. export control laws.

In November 2010, President Obama signed an Executive Order creating the Export Enforcement Coordination Center, or the E2C2. This multi-agency center is housed within HSI, and serves as the primary Government forum for the exchange of information, intelligence-related export enforcement.

The E2C2 enhances the United States' ability to combat illicit proliferation by working to coordinate investigative enforcement activities related to export control. The E2C2 is staffed with full-time personnel from HSI, as well as individuals detailed from other departments and agencies, including from the Department of State, Treasury, Defense, Justice, Commerce, Energy, and the ODNI to name a few.

There are a total of 18 partners that reside within the E2C2. Around their functions include coordinating and deconflicting our criminal and administrative enforcement actions in resolving interagency conflicts. They act as a primary point of contact between the enforcement authorities and the licensing authorities. They coordinate public outreach activities by law enforcement.

Finally, they are in the process of establishing a Government-wide statistical tracking capability. Additionally, as you know, ICE is the leading agency in the investigation of criminal intellectual property violations involving the illegal production, smuggling, and distribution of counterfeit and pirated products as well as the associated money-laundering violations.

The National Intellectual Property Rights Coordination Center, or the IPR Center, which is located in Arlington, Virginia brings together 20 Federal and international partners to provide a comprehensive response to IP theft. Outreach to the industry is also an important part of the IPR Center strategy.

To combat the theft of trade secrets, the IPR Center and the Department of Commerce have been hosting a series of intergovernmental meetings to identify the issues and the current U.S. Gov-

ernment response to trade theft. Then they plan to engage the industry representatives and obtain their input and support for enforcement efforts.

The IPR Center and Commerce are also providing outreach and training at the State and local level for retailers and brand owners. Through this effort, we are able to provide local rights holders and businesses the valuable insight on best practices, resources, initiatives that can help them combat IP violations, including trade secret theft.

HSI is working hard to address the proliferation of U.S. proprietary technology by foreign governments, and to ensure that the technology does not reach the wrong hands, and prosecute those who subvert the rule of law and threaten our National security.

We look forward to continuing our work with this subcommittee on this issue, and I thank you for involving me to testify today. I would be glad to answer any questions, when the time comes.

[The statement of Mr. Woods follows:]

PREPARED STATEMENT OF JOHN P. WOODS

JUNE 28, 2012

INTRODUCTION

Chairman Meehan, Ranking Member Higgins, and distinguished Members of the subcommittee: On behalf of Secretary Napolitano and Director Morton, I would like to thank you for the opportunity to discuss the efforts of U.S. Immigration and Customs Enforcement (ICE) to combat intellectual property (IP) and technology fraud by foreign governments. The theft of U.S. proprietary technology, including controlled dual-use technology and military-grade equipment, from unwitting U.S. companies is one of the most dangerous threats to National security. As I will discuss today, by maintaining investigative partnerships with other law enforcement agencies, both in the United States and internationally, ICE is at the forefront of the Nation's efforts to investigate these threats.

HSI's Counter-Proliferation Investigations Unit

ICE's Homeland Security Investigations (HSI) Directorate is the largest investigative program within the Department of Homeland Security (DHS), with an extensive portfolio of enforcement authorities. Notably, HSI special agents possess statutory authority to enforce more than 400 Federal laws. Specifically, HSI investigates a wide range of trade fraud, including IP theft, commercial fraud, and export violations. HSI special agents detect, disrupt, and dismantle cross-border criminal networks engaged in the smuggling of people, narcotics, bulk cash, weapons, and weapons-related components across our borders. HSI also has full statutory authority to investigate and enforce criminal violations of all U.S. export laws related to military items and controlled "dual-use" commodities (i.e., items with both commercial and military applications). Further, HSI has the capability to expand the scope of its investigations to its international offices situated throughout the world.

ICE leads the U.S. Government's efforts to prevent foreign adversaries from illegally obtaining U.S. military products and sensitive technology, including weapons of mass destruction and their components. HSI's Counter-Proliferation Investigations (CPI) Unit targets the trafficking and/or illegal export of conventional military equipment, firearms, controlled dual-use equipment and technology, and materials used to manufacture weapons of mass destruction, including chemical, biological, radiological, and nuclear materials. HSI special agents investigate illegal exports of military equipment and dual-use technology to embargoed countries, and significant financial and business transactions with proscribed countries and groups. Our HSI special agents also conduct export enforcement training for foreign law enforcement agencies, and provide outreach with private industry in the United States and internationally.

The primary goal of HSI CPI investigations is the detection and disruption of illegal exports before they, or the actors behind them, cause damage to the National security interests of the United States. HSI's export enforcement program uses a three-pronged approach: Detecting illegal exports, investigating potential violations,

and obtaining international cooperation to investigate leads abroad. HSI relies on specially-trained U.S. Customs and Border Protection officers stationed at ports of entry to inspect suspect export shipments. Following detection of a violation, HSI special agents deployed throughout the country initiate and pursue investigations to identify, arrest, and seek prosecution of offenders of the Arms Export Control Act of 1976, the Export Administration Act of 1979, the International Emergency Economic Powers Act, and other related statutes.

The international nature of counterproliferation networks and schemes requires a global investigative response. The HSI Office of International Affairs has 71 offices around the world that work to enlist the support of their host governments to initiate new investigative leads and to develop information in support of on-going domestic investigations.

In fiscal year 2011, HSI special agents initiated a total of 1,785 criminal investigations into possible export violations, made over 530 arrests, and obtained 487 indictments and 304 convictions for export-related criminal violations, more than any other Federal law enforcement agency (as reported by the Department of Justice). In addition, HSI agents conducted over 1,200 seizures of arms, military weaponry, and other sensitive commodities related to illegal export schemes. These efforts contributed to preventing sensitive U.S. technologies and weapons from falling into the wrong hands.

Project Shield America (PSA)

One of the most effective tools HSI special agents use as part of HSI's larger counter-proliferation strategy is our industry outreach program, Project Shield America (PSA). Through this program, HSI special agents conduct outreach to manufacturers and exporters of strategic commodities to educate them on U.S. export control laws, discuss export licensing issues and requirements, identify "red flag" indicators used in illegal procurement, and identify the Government agencies responsible for the licensing of export controlled commodities and technology. As of 2011, HSI agents have delivered over 20,000 outreach presentations to private industry and other entities as part of the PSA program.

Export Enforcement Coordination Center (E2C2)

A part of the President's Export Control Reform Initiative is to improve law enforcement coordination to investigate violations of U.S. export control laws. In November 2010, President Obama signed an Executive Order creating the Export Enforcement Coordination Center (E2C2)—a multi-agency center housed within HSI that serves as the primary Government forum for the exchange of information and intelligence related to export enforcement. Operational since April of this year, E2C2 enhances the United States' ability to combat illicit proliferation by working to coordinate investigative and enforcement activities related to export control.

The E2C2 is staffed with full-time personnel from HSI, as well as individuals detailed from other departments and agencies including the Departments of State, Treasury, Defense (DoD), Justice, Commerce, Energy, the Office of the Director of National Intelligence, and other Executive Branch departments, agencies, or offices as designated by the President. Specifically, the functions of the E2C2 include:

- Coordinating the deconfliction of criminal and administrative enforcement actions and resolving conflicts that have not been otherwise resolved in the field;
- Acting as the primary point of contact between enforcement authorities and agencies engaged in export licensing;
- Coordinating law enforcement public outreach activities related to U.S. export controls; and
- Establishing Government-wide statistical tracking capabilities for U.S. export enforcement activities.

The E2C2 replaced HSI's National Export Enforcement Coordination Network (NEECN), which led coordination among DHS components to address challenges inherent with dismantling transnational procurement networks. Unlike the NEECN, the Executive Order requires E2C2 participation by law enforcement and the intelligence community (IC).

CPI Centers

Faced with increasingly sophisticated global procurement networks, HSI has established and implemented CPI Centers throughout the United States to utilize CPI resources in the field strategically. The CPI Centers are intended to serve as a regional HSI resource for manpower, expertise, de-confliction, undercover operational support, and/or other CPI assistance that HSI offices may require. This concept allows for dedicated and experienced HSI special agents to be strategically placed in high-risk domestic areas to improve HSI's ability to combat illegal exports and illicit procurement networks that pose a threat to the United States.

Geographically, CPI Centers are selected based on criteria including significant cases and statistics, threat assessments in respective areas of responsibility, and proximity to DoD and other U.S. Government agencies involved in export enforcement. ICE currently has 12 CPI Centers located throughout the United States.

National Intellectual Property Rights Center

ICE is a leading agency in the investigation of criminal intellectual property violations involving the illegal production, smuggling, and distribution of counterfeit and pirated products, as well as associated money-laundering violations. Led by ICE, the National Intellectual Property Rights Coordination Center (IPR Center), located in Arlington, Virginia, brings together 20 Federal and international partners to leverage resources, skills, and authorities to provide a comprehensive response to IP theft.

The mission of the IPR Center is to address the theft of innovation that threatens U.S. economic stability and National security, undermines the competitiveness of U.S. industry in world markets, and places the public's health and safety at risk. The entry of goods into the United States is an integral part of the economic health of our Nation. However, with the growth of international trade comes an increased risk of border security compromises, including threats to National security and economic crime.

IPR Center Outreach

Outreach to industry is an important part of the IPR Center's strategy. To combat the theft of trade secrets, the IPR Center and the Department of Commerce (DOC) have been hosting a series of intra-governmental meetings to identify the issues and the current U.S. Government response to trade secret theft, and then plan to engage with industry representatives to obtain their input and support in these efforts.

The IPR Center has further enhanced its collaboration with the DOC to provide outreach and training at the State and local level for retailers and brand owners. In collaboration with the U.S. Export Assistance Centers, these outreach and awareness-raising efforts are planned to precede or follow selected IPR Center training events. Through this effort, DOC and the IPR Center, along with other U.S. Government agencies and industry, are able to provide local rights holders and businesses with valuable insight on best practices, resources, and initiatives that can help them combat IP violations, including trade secret theft.

CONCLUSION

HSI special agents are working tirelessly to combat the proliferation of U.S. proprietary technology by foreign governments, ensure that this technology does not reach the wrong hands, and prosecute those who subvert the rule of law and threaten our National security. We look forward to continuing to work with the subcommittee on this issue.

Thank you once again for the opportunity to appear before you today. I would be pleased to answer any questions.

Mr. LONG. The Chairman now recognizes—oops. Thank you, Mr. Woods.

The Chairman now recognizes Mr. Figliuzzi to testify.

STATEMENT OF C. FRANK FIGLIUZZI, ASSISTANT DIRECTOR, COUNTERINTELLIGENCE DIVISION, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. FIGLIUZZI. Good morning, Chairman Long and Ranking Member Higgins, and Members of the subcommittee. Thank you for the opportunity to testify before you today. For the past year-and-a-half I have had the privilege of leading the FBI's counterintelligence division.

Our mission is to identify, disrupt, and defeat the efforts of foreign intelligence services operating inside a United States. To put it simply, the FBI is in the spy-catching business, and today I can tell you that our business is booming. This is an appropriate time to address economic espionage: The unauthorized acquisition of business trade secrets or proprietary information and the illegal transfer of technology.

With each year, foreign intelligence services and their collectors become more sophisticated in their methods to undermine American business and erode what gives America our leading edge—our ability to innovate. In the FBI's pending caseload, just this fiscal year economic espionage has cost the American economy more than $13 billion. The health of America's companies is vital to our economy, and our economic is a matter of National security.

But the FBI, with our partner agencies, is making strides in disrupting economic espionage plots. This year, we have surpassed last year's statistics by achieving 10 arrests, 21 indictments, and 9 convictions for economic espionage-related crimes. As the FBI's economic espionage caseload is growing, so is the percentage of our cases attributed to an insider threat coming from trusted employees and contractors, or former employees and contractors.

This threat, of course, is not new. But it is becoming more prevalent. In this time of global economic uncertainty, it is lucrative for an employee to steal our technology and offer it to the highest bidder. Foreign nations know that it is always cheaper to steal U.S. technology than it is to research and develop it themselves.

On May 11, 2012 the FBI initiated a public awareness campaign regarding an increased targeting of unclassified trade secrets across all American industries and sectors. Our website, *www.fbi.gov,* includes many resources to help counter this threat.

The illegal transfer of U.S. technology is a second grave threat to our National security. The FBI is seeing an expansion of weapons proliferation cases involving U.S.-acquired components. These are components exported from American companies initially headed to someplace they are allowed to be but, ultimately, destined for someplace they should never be.

The FBI's counterproliferation center, that identifies and disrupts networks of WMD activity, has tripled its disruptions of illegal transfers of technology since fiscal year 2011, including making more than a dozen arrests in the last year. Two case examples illustrate our successes in working alongside our U.S. law enforcement and intelligence community partners.

In the first case, an Iranian proliferator used shell companies worldwide to supply Iran with military- and defense-related equipment. In 4 years, FBI cases helped interdict metal shipments headed to Iran which would have been the equivalent of more than 80 ballistic missiles.

In the second case, another Iranian proliferation network obtained dual-use equipment from unwitting U.S. companies and shipped them to intermediary front companies in Asian nations before ultimately rerouting the shipments to Iran. More than a dozen of these components have been recovered as part of improvised explosive devices used against American servicemembers in Iraq from 2008 to 2011.

The threat of economic espionage and illegal transfers of technology are not emerging threats on the horizon; they are with us right now. As long as America has what other nations want, and as long as there are foreign intelligence services working to get it, we will continue to see these types of threats.

We are producing results as a result of our robust Government, business, and academic outreach partnerships, including partner-

ships among the agencies represented today at this hearing. We are all making it more difficult and less lucrative for individuals and entities to carry out the illegal taskings of foreign governments, and hardening our defenses against those who would so us harm.

Thank you for the opportunity to speak to you today, and I would be happy to answer your questions.

[The statement of Mr. Figliuzzi follows:]

PREPARED STATEMENT OF C. FRANK FIGLIUZZI

JUNE 28, 2012

Good morning Chairman Meehan, Ranking Member Higgins, and Members of the subcommittee. Thank you for the opportunity to testify before you today. For the past year-and-a-half, I have had the privilege of leading the FBI's Counterintelligence Division ("CD"). Our mission is to identify, disrupt, and defeat the efforts of foreign intelligence services operating inside the United States. In the FBI's pending case load for the current fiscal year, economic espionage losses to the American economy total more than $13 billion. The health of America's companies is vital to our economy, and our economy is a matter of National security. But the FBI, with our partners, is making strides in disrupting economic espionage plots. In just the last 4 years, the number of arrests the FBI has made associated with economic espionage has doubled; indictments have increased five-fold; and convictions have risen eight-fold. In just the current fiscal year, the FBI has made 10 arrests for economic espionage-related charges; Federal courts have indicted 21 of our subjects (including indictments of five companies), and convicted nine defendants. In the current fiscal year so far, we have already surpassed the statistics recorded for fiscal year 2011 and expect them to continue to rise. With each year, foreign intelligence services and their collectors become more creative and more sophisticated in their methods to undermine American business and erode the one thing that most provides American business its leading edge—our ability to innovate.

As the FBI's economic espionage caseload is growing, so is the percentage of cases attributed to an Insider Threat, meaning that, individuals currently (or formerly) trusted as employees and contractors are a growing part of the problem.

According to a February 2012 indictment, several former employees with more than 70 combined years of service to the company were convinced to sell trade secrets to a competitor in the People's Republic of China ("PRC"). Entities owned by the PRC government sought information on the production of titanium dioxide, a white pigment used to color paper, plastics, and paint. The PRC government tried for years to compete with DuPont Corporation, which holds the largest share of a $12 billion annual market in titanium dioxide. Five individuals and five companies were commissioned by these PRC state-owned enterprises collaborate in an effort to take DuPont's technology to the PRC and build competing titanium dioxide plants, which would undercut DuPont revenues and business. Thus far, three co-conspirators have been arrested and one additional co-conspirator has pled guilty in Federal court. This case is one of the largest economic espionage cases in FBI history.

The Insider Threat, of course, is not new, but it's becoming more prevalent for a host of reasons, including

- The pervasiveness of employee financial hardships during economic difficulties;
- The global economic crisis facing foreign nations, making it even more attractive, cost-effective, and worth the risk to steal technology rather than invest in research and development;
- The ease of stealing anything stored electronically, especially when one has legitimate access to it; and
- The increasing exposure to foreign intelligence services presented by the reality of global business, joint ventures, and the growing international footprint of American firms.

To address the evolving Insider Threat, the FBI has become more proactive to prevent losses of information and technology. CD continues expanding our outreach and liaison alliances to Government agencies, the defense industry, academic institutions, and, for the first time, to the general public, because of an increased targeting of unclassified trade secrets across all American industries and sectors.

On May 11, 2012, the FBI launched a media campaign highlighting the Insider Threat relating to economic espionage. This campaign included print and television

interviews, billboards along busy commuter corridors in nine leading research areas Nation-wide, and public information on the FBI website. Through this campaign, the FBI hopes to reach the public and business communities by explaining how the Insider Threat affects a company's operations and educating them on how to detect, prevent, and respond to threats to their organizations' proprietary information. Perhaps the most important among these is identifying and taking defensive measures against employees stealing trade secrets.

A recent case underscores the value of the FBI and private companies working together to stop economic espionage and prevent financial losses or breaches of National security. An employee at a Utah company noticed a co-worker download the recipe for manufacturing a proprietary chemical and email it to his personal email account. After this suspicious activity was reported, the company opened its own investigation into the matter and learned that the employee had shared the manufacturing secret with an individual associated with a foreign chemical company. Because of an FBI presentation about economic espionage, company executives called the FBI, and the employee was arrested and charged within 10 days. If businesses, universities, and law enforcement continue to partner together, we can track, apprehend, and prosecute many more individuals suspected of economic espionage.

A second grave threat to our National security is the illegal transfer of U.S. technology. The FBI is seeing an expansion of weapons proliferation cases involving U.S.-acquired components. These are components exported from American companies, initially headed to someplace they're allowed to be, but ultimately destined for someplace they should never be. The FBI's Counterproliferation Center (CPC), which identifies and disrupts networks of weapons of mass destruction (WMD) activity, is responsible for pursuing cases of illegal technology transfer, whether the technology is intended for WMDs or other uses. The CPC has tripled its disruptions of illegal transfers of technology since fiscal year 2011. We have made more than a dozen arrests since the CPC's inception in July 2011, including the arrests of multiple subjects on the Central Intelligence Agency's Top Ten Proliferators List. The CPC has also surpassed statistics recorded for fiscal year 2011 and in fiscal year 2012 (to date).

One example of this sort of case involved an Iranian proliferation network with associates in Hong Kong, Taiwan, Singapore, and Malaysia, and particularly highlights our partnership with the Department of Commerce's Office of Export Enforcement and Homeland Security investigations. The network leader targeted dual-use electronic equipment including radio frequency modules. The target obtained this equipment from unwitting U.S. companies and shipped them to intermediary front companies in East Asia before ultimately rerouting the shipments to Iran. Over a dozen of these components have been recovered in caches of improvised explosive devices ("IEDs") or recovered as part of the remote detonation systems of the pre- and post-blast IEDs used against American soldiers in Iraq from 2008–2011. Four co-conspirators in Singapore have been arrested and extradition proceedings to the United States to stand trial are on-going. One U.S. co-conspirator, who worked in research and development at the company manufacturing and shipping these items, pled guilty in Federal court this January.

The answer to the threat lies, in part, on the partnerships represented at this hearing. Acting together, we are stronger than when we act alone and are producing results. As we continue our investigative and prosecutorial efforts we make it more painful for individuals and entities to carry out missions related to economic espionage. And as we strengthen and expand public awareness of the threat through our alliances with business and academia, we harden our defenses against those who would do us harm.

Again, thank you for the opportunity to speak with you today. I would be pleased to answer any questions.

Mr. LONG. Thank you, Mr. Figliuzzi.

The Chairman now recognizes Mr. Wilshusen to testify.

STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Long, Ranking Member Higgins, and Members of the subcommittee, thank you for the opportunity to testify at today's hearing on the threat of economic espionage facing the United States.

This threat is not new. In April, 1992 we testified that the theft of U.S. proprietary information or technology by foreign companies has long been a part of the competitive business environment. We also testified that the unauthorized acquisition of U.S. proprietary and other information by foreign governments to advance their country's economic position was growing.

Today, this threat continues to grow. The United States, a leader in innovation and technological research and development, remains a prime target. In addition, the increasing dependence on network IT systems and the use of cyberspace have vastly enhanced the reach and potential impact of such threats by making it possible for hostile actors to quickly steal massive amounts of information while remaining anonymous and difficult to detect.

Mr. Chairman, I will describe some of the cyber threats, reported incidents affecting our Nation's systems, IT security safeguards available for helping to reduce these risks, and the roles of key Federal entities in supporting the protection of intellectual property. But before I do, Mr. Chairman, if I may I would like to recognize several members of my team who were instrumental in developing this statement.

With me today is Mike Gilmore and Angelique Lawrence. Back at the office, Lee McCracken, Brad Becker, and Kush Malhotra were very helpful.

Mr. Chairman, the Nation faces an evolving array of cyber-based threats from a variety of sources. These sources include foreign nations, business competitors, criminal groups, hackers, and corrupt insiders engaged in criminal activities such as fraud, computer extortion, and economic and industrial espionage, among others.

They vary in their terms of capabilities, willingness to act, and motives, which can include seeking monetary gain and pursuing economic, political, or military advantage. Moreover, they have a variety of attack techniques that can be used to view, exfiltrate, and modify valuable information. The magnitude of the threat is compounded by the ever-increasing sophistication of cyber attack techniques, such as attacks that may combine multiple exploits.

Reported attacks involving private-sector and Government systems occur daily and demonstrate that their impact can be serious. For example, consumers could suffer privacy and financial loss from identity theft and on-line scams. Private companies could lose their competitive advantage and market value from the cyber theft of an intellectual property or business proprietary information.

Essential Government functions and critical infrastructure services could be impaired or disrupted. To protect against these threats, a variety of security controls and practices are available. These include technical controls such as those that manage access to systems, ensure system integrity, and encrypt sensitive data.

Risk management and strategic planning are key practices that organizations undertake to improve their overall security posture and reduce their exposure to cyber risk. Effective public-private partnerships can facilitate information-sharing about cyber threats and countermeasures. Multiple Federal agencies have roles in supporting the protection of intellectual property rights, such as the Departments of Commerce, Justice, and Homeland Security.

For example, components within the Justice Department, including the FBI, are dedicated to fighting computer-based threats to intellectual property. In addition, both Congress and the administration have established interagency mechanisms to better coordinate the protection of intellectual property.

Ensuring the effective coordination among these efforts will be imperative for enhancing the economic security of the United States. In summary, the on-going efforts to steal U.S. intellectual property and other sensitive information are exacerbated by the ever-increasing prevalence and sophistication of cyber threats facing the Nation.

Recently-reported incidents show that such actions can have serious consequences not only on individual businesses, but on private citizens and the economy as a whole. Effective coordination among Federal agencies, as well as robust public-private partnerships, are essential elements of any Nation-wide effort to protect America's businesses and economic security from cyber-based threats.

Mr. Chairman, Ranking Member Higgins, this concludes my statement. I would be pleased to answer any questions you may have.

[The statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

Chairman Meehan, Ranking Member Higgins, and Members of the subcommittee: Thank you for the opportunity to testify at today's hearing on the threat of economic espionage facing U.S. businesses.

The threat of economic espionage[1] is not new. In April 1992, we testified that the theft of U.S. proprietary information or technology by foreign companies has long been a part of the competitive business environment.[2] We also testified that the unauthorized acquisition of U.S. proprietary or other information by foreign governments to advance their countries' economic position was growing.

Today, this threat continues to grow. According to the Federal Bureau of Investigation (FBI), the theft of intellectual property (IP)[3]—products of human intelligence and creativity—is a growing threat which is heightened by the rise of the use of digital technologies.[4] The increasing dependency upon information technology (IT) systems and networked operations pervades nearly every aspect of our society. In particular, increasing computer interconnectivity—most notably growth in the use of the internet—has revolutionized the way that our Government, our Nation, and much of the world communicate and conduct business. While bringing significant benefits, this dependency can also create vulnerabilities to cyber-based threats. Cyber attacks are one way that threat actors—whether nations, companies, or criminals—can target the intellectual property and other sensitive information of Federal agencies and American businesses. According to the Office of the National Counterintelligence Executive, sensitive U.S. economic information and technology are targeted by intelligence services, private-sector companies, academic and research in-

---

[1] According to the Office of the National Counterintelligence Executive, economic espionage occurs when an actor, knowing or intending that his or her actions will benefit any foreign government, instrumentality, or agent, knowingly: (1) Steals, or without authorization appropriates, carries away, conceals, or obtains by deception or fraud a trade secret; (2) copies, duplicates, reproduces, destroys, uploads, downloads, or transmits that trade secret without authorization; or (3) receives a trade secret knowing that the trade secret had been stolen, appropriated, obtained or converted without authorization. See *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011* (October 2011).

[2] GAO, *Economic Espionage: The Threat to U.S. Industry,* Testimony before the Subcommittee on Economic and Commercial Law, Committee on the Judiciary, House of Representatives, GAO/T–OSI–92–6 (April 29, 1992).

[3] Intellectual property is a category of legal rights that grants owners certain exclusive rights to intangible assets or products of the human intellect, such as inventions; literary and artistic works; and symbols, names, images, and design.

[4] See the FBI's website on cybercrime and intellectual property theft at *http://www.fbi.gov/about-us/investigate/cyber/ipr/ipr.*

stitutions, and citizens of dozens of countries.[5] To help address this threat, Federal agencies have a key role to play in law enforcement, deterrence, and information sharing. Underscoring the importance of this issue, we have designated Federal information security as a high-risk area since 1997 and in 2003 expanded this area to include protecting computerized systems supporting our Nation's critical infrastructure.[6]

In my testimony today, I will describe: (1) Cyber threats facing the Nation's systems, (2) reported cyber incidents and their impacts, (3) security controls and other techniques available for reducing risk, and (4) the responsibilities of key Federal entities in support of improving the protection of intellectual property. In preparing this statement in June 2012, we relied on our previous work in these areas. (Please see the related GAO products in appendix II.) These products contain detailed overviews of the scope and methodology we used. We also reviewed relevant reports from the Department of Justice and Office of the National Counterintelligence Executive, and information on security incidents, including those involving economic espionage, from the U.S. Computer Emergency Readiness Team (US–CERT), media reports, and other publicly available sources. The work on which this statement is based was conducted in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

As computer technology has advanced, both Government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transmit sensitive and proprietary information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services. In addition, the internet has grown increasingly important to American business and consumers, serving as a medium for hundreds of billions of dollars of commerce each year.

Consequently, ineffective information security controls can result in significant risks, including:

- loss or theft of resources, including money and intellectual property;
- inappropriate access to and disclosure, modification, or destruction of sensitive information;
- use of computer resources for unauthorized purposes or to launch attacks on other computers' systems;
- damage to networks and equipment;
- loss of business due to lack of customer confidence; and
- increased costs from remediation.

THE NATION FACES AN EVOLVING ARRAY OF CYBER-BASED THREATS

Cyber-based threats are evolving and growing and arise from a wide array of sources. These sources include business competitors, corrupt employees, criminal groups, hackers, and foreign nations engaged in espionage and information warfare. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Table 1 shows common sources of cyber threats.

[5] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.*

[6] See, most recently, GAO, *High-Risk Series: An Update,* GAO–11–278 (Washington, DC: February 2011).

TABLE 1.—SOURCES OF CYBERSECURITY THREATS

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Business competitors	Companies that compete against or do business with a target company may seek to obtain sensitive information to improve their competitive advantage in various areas, such as pricing, manufacturing, product development, and contracting.
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, on-line fraud, and computer extortion.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled or corrupt organization insider is a source of computer crime including economic espionage. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly-trained employees who may inadvertently introduce malware into systems.
International corporate spies.	International corporate spies pose a threat to the United States through their ability to conduct economic and industrial espionage* and large-scale monetary theft and to hire or develop hacker talent.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities, including economic espionage directed against U.S. businesses. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives.

TABLE 1.—SOURCES OF CYBERSECURITY THREATS—Continued

Threat source	Description
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or malware authors.	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several notable destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten National security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

*According to the Office of the National Counterintelligence Executive, industrial espionage, or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner. See *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.*

Source.—GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, National Institute of Standards and Technology, and the Software Engineering Institute's CERT® Coordination Center.

These sources of cyber threats make use of various techniques, or exploits, to adversely affect an organization's computers, software, or networks, or to intercept or steal valuable or sensitive information. Table 2 provides descriptions of common types of cyber exploits.

TABLE 2.—TYPES OF CYBER EXPLOITS

Type of Exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service.	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Logic bombs	A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.

TABLE 2.—TYPES OF CYBER EXPLOITS—Continued

Type of Exploit	Description
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured Query Language (SQL) injection.	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks.
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed time frame between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports.

Cyberspace—where much business activity and the development of new ideas often take place—amplifies these threats by making it possible for malicious actors to quickly steal and transfer massive quantities of data while remaining anonymous and difficult to detect.[7] For example, cyber attackers do not need to be physically close to their victims, technology allows attacks to easily cross State and National borders, attacks can be carried out at high speed and directed at a number of victims simultaneously, and cyber attackers can more easily remain anonymous. Moreover, the use of these and other techniques is becoming more sophisticated, with attackers using multiple or "blended" approaches that combine two or more techniques. Using such techniques, threat actors may target individuals, resulting in loss of privacy or identity theft; businesses, resulting in the compromise of proprietary information or intellectual property; critical infrastructures, resulting in their disruption or destruction; or Government agencies, resulting in the loss of sensitive information and damage to economic and National security.

REPORTED CYBER-INCIDENTS ILLUSTRATE SERIOUS RISK TO THE SECURITY OF INTELLECTUAL PROPERTY AND OTHER SENSITIVE ECONOMIC INFORMATION

Reports of cyber incidents affecting both public and private institutions are widespread. The U.S. Computer Emergency Readiness Team (US–CERT) receives computer security incident reports from Federal agencies, State and local governments,

[7] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.*

commercial enterprises, U.S. citizens, and international computer security incident response teams. In its fiscal year 2011 report to Congress on implementation of the Federal Information Security Management Act of 2002, the Office of Management and Budget reported that US–CERT received over 100,000 total incident reports in fiscal year 2011. Over half of these (about 55,000) were phishing exploits; other categories of incidents included virus/Trojan horse/worm/logic bombs; malicious websites; policy violations; equipment theft or loss; suspicious network activity; attempted access; and social engineering.

Private-sector organizations have experienced a wide range of incidents involving data loss or theft, economic loss, computer intrusions, and privacy breaches, underscoring the need for improved security practices. The following examples from news media and other public sources illustrate that a broad array of information and assets remain at risk.

- In March 2012, it was reported that a security breach at Global Payments, a firm that processed payments for Visa and Mastercard, could compromise the credit- and debit-card information of millions of Americans. Subsequent to the reported breach, the company's stock fell more than 9 percent before trading in its stock was halted. Visa also removed the company from its list of approved processors.
- In March 2012, it was reported that Blue Cross Blue Shield of Tennessee paid out a settlement of $1.5 million to the U.S. Department of Health and Human Services arising from potential violations stemming from the theft of 57 unencrypted computer hard drives that contained protected health information of over 1 million individuals.
- In April 2011, Sony disclosed that it suffered a massive breach in its video game on-line network that led to the theft of personal information, including the names, addresses, and possibly credit card data belonging to 77 million user accounts.
- In February 2011, media reports stated that computer hackers had broken into and stolen proprietary information worth millions of dollars from the networks of six U.S. and European energy companies.
- A retailer reported in May 2011 that it had suffered a breach of its customers' card data. The company discovered tampering with the personal identification number (PIN) pads at its checkout lanes in stores across 20 States.
- In mid-2009 a research chemist with DuPont Corporation reportedly downloaded proprietary information to a personal e-mail account and thumb drive with the intention of transferring this information to Peking University in China and also sought Chinese government funding to commercialize research related to the information he had stolen.
- Between 2008 and 2009, a chemist with Valspar Corporation reportedly used access to an internal computer network to download secret formulas for paints and coatings, reportedly intending to take this proprietary information to a new job with a paint company in Shanghai, China.
- In December 2006, a product engineer with Ford Motor Company reportedly copied approximately 4,000 Ford documents onto an external hard drive in order to acquire a job with a Chinese automotive company.

These incidents illustrate the serious impact that cyber threats can have on, among other things, the security of sensitive personal and financial information and proprietary information and intellectual property. While these effects can be difficult to quantify monetarily, they can include any of the following:

- For consumers or private citizens: Identity theft or compromise of personal and economic information and costs associated with lower-quality counterfeit or pirated goods.
- For business: Lost sales, lost brand value or damage to public image, cost of intellectual property protection, and decreased incentive to invest in research and development.
- For the economy as a whole: Lower economic growth due to reduced incentives to innovate and lost revenue from declining U.S. trade with countries that have weak IP rights regimes.

SECURITY CONTROLS AND OTHER TECHNIQUES CAN REDUCE VULNERABILITY TO CYBER-BASED ATTACKS

The prevalence of cyber threats and the risks they pose illustrate the need for security controls and other actions that can reduce organizations' vulnerability to such attacks. As we have reported, there are a number of cybersecurity technologies that can be used to better protect systems from cyber attacks, including access control technologies, system integrity technologies, cryptography, audit and monitoring

tools, and configuration management and assurance technologies.[8] In prior reports, we have made hundreds of recommendations to Federal agencies to better protect their systems and cyber-reliant critical infrastructures. Table 3 summarizes some of the common cybersecurity technologies, categorized by the type of security control they help to implement.

[8] GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection,* GAO–04–321 (Washington, DC: May 28, 2004).

TABLE 3.—COMMON CYBERSECURITY TECHNOLOGIES

Category	Technology	What it does
Access control:		
Boundary protection	Firewalls	Control access to and from a network or computer.
Authentication	Biometrics	Uses human characteristics, such as fingerprints, irises, and voices, to establish the identity of the user.
Authorization	User rights and privileges	Allow or prevent access to data and systems and actions of users based on the established policies of an organization.
System integrity	Antivirus software	Provides protection against malicious code, such as viruses, worms, and Trojan horses.
Cryptography	Digital signatures and certificates	Use public key cryptography to provide: (1) Assurance that both the sender and recipient of a message or transaction will be uniquely identified, (2) assurance that the data have not been accidentally or deliberately altered, and (3) verifiable proof of the integrity and origin of the data.
	Virtual private networks	Allow organizations or individuals in two or more physical locations to establish network connections over a shared or public network, such as the internet, with functionality that is similar to that of a private network using cryptography.
Audit and monitoring	Intrusion detection systems	Detect inappropriate, incorrect, or anomalous activity on a network or computer system.
	Intrusion prevention systems	Build on intrusion detection systems to detect attacks on a network and take action to prevent them from being successful.
	Computer forensics tools	Identify, preserve, extract, and document computer-based evidence.
Configuration management and assurance.	Policy enforcement applications	Enable system administrators to engage in centralized monitoring and enforcement of an organization's security policies.
	Network management	Allow for the control and monitoring of networks, including management of faults, configurations, performance, and security.

Scanners	Analyze computers or networks for security vulnerabilities.
Continuity of operations tools	Provide a complete backup infrastructure to maintain availability in the event of an emergency or during planned maintenance.
Patch management	Acquires, tests, and applies multiple patches to one or more computer systems.

Source: GAO analysis.

In addition, the use of an overall cybersecurity framework can assist in the selection of technologies to protect an organization against cyber attacks. Such a framework includes:

- determining the business requirements for security;
- performing risk assessments;
- establishing a security policy;
- implementing a cybersecurity solution that includes people, process, and technology to mitigate identified security risks; and
- continuously monitoring and managing security.

Risk assessments, which are central to this framework, help organizations determine which assets are most at risk and to identify countermeasures to mitigate those risks. Risk assessment is based on a consideration of threats and vulnerabilities that could be exploited to inflict damage.

Even with such a framework, there often are competing demands for cybersecurity investments. For example, for some companies, mitigating physical risks may be more important than mitigating cyber risks. Further, investing in cybersecurity technologies needs to make business sense. It is also important to bear in mind the limitations of some cybersecurity technologies and to be aware that their capabilities should not be overstated. Technologies do not work in isolation. Cybersecurity solutions make use of people, process, and technology. Cybersecurity technology must work within an overall security process and be used by trained personnel. We have also emphasized the importance of public-private partnerships for sharing information and implementing effective cybercrime prevention strategies.[9]

Similarly, the Office of the National Counterintelligence Executive has identified a series of "best practices in data protection strategies and due diligence for corporations."[10] These include developing an information strategy; insider threat programs and awareness; effective data management; network security, auditing, and monitoring; and contingency planning.

KEY FEDERAL AGENCIES HAVE RESPONSIBILITIES FOR PROTECTING INTELLECTUAL PROPERTY

Multiple Federal agencies undertake a wide range of activities in support of IP rights. Some of these agencies are the Departments of Commerce (including the U.S. Patent and Trademark Office), State, Justice (including the FBI), Health and Human Services, and Homeland Security; the U.S. Trade Representative; the U.S. Copyright Office; and the U.S. International Trade Commission. In many cases, IP-related efforts represent a small part of the agencies' much broader missions.

A smaller number of agencies and their components are involved in investigating IP violations and enforcing U.S. IP laws. For example, the Department of Justice's (DOJ) U.S. attorneys offices, Criminal Division, and the FBI investigate and prosecute Federal IP crimes. DOJ established the Computer Hacking and Intellectual Property program, which consists of specially-trained assistant U.S. attorneys to pursue IP cases. Each of the 93 U.S. attorneys offices throughout the country have assistant U.S. attorneys designated as Computer Hacking and Intellectual Property coordinators, who are available to work on IP cases. In addition, DOJ has created Computer Hacking and Intellectual Property units in 25 U.S. attorneys offices with histories of large IP case loads. DOJ's Computer Crime and Intellectual Property Section—based in Washington, DC—consists of prosecutors devoted to enforcing computer crime and IP laws. Computer Crime and Intellectual Property Section attorneys prosecute cases, assist prosecutors and other investigative agents in the field, and help develop and implement an overall criminal enforcement strategy. The FBI's Cyber Division oversees the bureau's IP enforcement efforts; though not all of its IP investigations are cyber-related.

Over the years, Congress and the administration have created interagency mechanisms to coordinate Federal IP law enforcement efforts. These include the National Intellectual Property Law Enforcement Coordination Council (NIPLECC), created in 1999 to coordinate U.S. law enforcement efforts to protect and enforce IP rights in the United States and abroad and the Strategy for Targeting Organized Piracy initiative, created by the President in 2004 to target cross-border trade in tangible goods and strengthen U.S. Government and industry IP enforcement action. In December 2004, Congress passed legislation to enhance NIPLECC's mandate and created the position of the Coordinator for International Intellectual Property Enforce-

[9] GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats,* GAO–07–705 (Washington, DC: June 22, 2007).

[10] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.*

ment, located within the Department of Commerce, to lead NIPLECC. In November 2006 we reported that NIPLECC continued to face persistent difficulties, creating doubts about its ability to carry out its mandate.[11] We also noted that while the Strategy for Targeting Organized Piracy had brought attention and energy to IP efforts within the U.S. Government, it had limited usefulness as a tool to prioritize, guide, implement, and monitor the combined efforts of multiple agencies.

In 2008, Congress passed the Prioritizing Resources and Organization for Intellectual Property Act (PRO–IP Act), which, among other things, created the position of the Intellectual Property Enforcement Coordinator (IPEC) to serve within the Executive Office of the President. The duties of the coordinator outlined in the act include specific efforts to enhance interagency coordination, such as the development of a comprehensive joint strategic plan. The act also required the Attorney General to devote additional resources to IP enforcement and undertake other IP-enforcement-related efforts. In October 2010, we noted that DOJ and FBI officials and Office of the IPEC staff reported taking many actions to implement the requirements of the PRO–IP Act.[12] Moreover, the IPEC coordinated with other Federal entities to deliver the 2010 Joint Strategic Plan on Intellectual Property Enforcement to Congress and the public. We reported that the plan addressed the content requirements of the act, but that enhancements were needed, such as identifying responsible departments and entities for all action items and estimates of resources needed to carry out the plan's priorities. Accordingly, we recommended that the IPEC take steps to ensure that future strategic plans address these elements. IPEC staff generally concurred with our findings and recommendations.

In summary, the on-going efforts to steal U.S. companies' intellectual property and other sensitive information are exacerbated by the ever-increasing prevalence and sophistication of cyber-threats facing the Nation. Recently reported incidents show that such actions can have serious impact not only on individual businesses, but on private citizens and the economy as a whole. While techniques exist to reduce vulnerabilities to cyber-based threats, these require strategic planning by affected entities. Moreover, effective coordination among Federal agencies responsible for protecting IP and defending against cyber-threats, as well as effective public-private partnerships, are essential elements of any Nation-wide effort to protect America's businesses and economic security.

Chairman Meehan, Ranking Member Higgins, and Members of the subcommittee, this concludes my statement. I would be happy to answer any questions you have at this time.

Mr. LONG. Thank you, Mr. Wilshusen for your testimony today, and also for acknowledging your coworkers. I know that that is where a lot of the work gets done up here, and they go unrecognized. So I appreciate that because I know, on a personal level, that it is very important in my office and most offices around here. Like I say, a pat on the back never hurts anybody.

I now recognize myself for a round of questioning. Dr. Graham, in April the Commerce Department released a report showing that intellectual property-intensive industries contributed $5 trillion and 40 million jobs to the economy in 2010. Can you speak to the threat that economic espionage poses to various sectors of the economy, and provide some examples of industries that are targeted by foreign actors?

Mr. GRAHAM. Thank you, Mr. Chairman. I am happy to do so. Indeed, what this report does and why I came here today to testify was to essentially set the stage, and to speak to what is at stake here.

So, you know, indeed the report did identify the most intellectual property-intensive industries in the U.S. economy, with the statistics that I cited earlier; 35 percent of GNP, approximately 28 percent of employment throughout the economy.

---

[11] GAO, *Intellectual Property: Strategy for Targeting Organized Piracy (STOP) Requires Changes for Long-term Success,* GAO–07–74 (Washington, DC: Nov. 8, 2006).

[12] GAO, *Intellectual Property: Agencies Progress in Implementing Recent Legislation, but Enhancements Could Improve Future Plans,* GAO–11–39 (Washington, DC: Oct. 13, 2010).

It stands to reason that the threats associated with, created by, espionage would be particularly biting in these industries, since so much of their competitive advantage is built upon and based upon these intangible assets that they are building.

There has been significant study before, particularly on the area of how important these intellectual property protections are for U.S. companies in capturing and maintaining competitive advantage. What we see time and time again, from the way in which these companies innovate and what they do with their innovations and the economic fruits and the economic benefits that flow to Americans and American employees from these innovations—are disrupted when those companies, when those firms, can't get access to these intellectual property protections.

So at the end of the day we have to say that, you know, when we are looking at industries—from pharmaceuticals to machinery to chemicals to semiconductors to electronics—widely throughout the economy the threat associated with the undermining of the ability of these companies to maintain those rights and expect that those rights are going to be adequately protected will be significant to the economy.

The estimates that have been put out of $13 billion, they seem to be perfectly appropriate estimates. But, of course, what those estimates must be, ultimately, are an under-count. Because what we can never count are the benefits associated to innovation that never happened because innovators are less likely to create their innovations, to expend those resources and investments, because they fear that what they are going to get at the end is an unprotectable product.

So, you know, indeed, at the end of the day, these are real threats. They have a real impact on what is going on. The pie, as I have said before, is incredibly larger.

Mr. LONG. Okay, thank you.

Assistant Director Figliuzzi, in an interview with the *San Francisco Chronicle* you stated that the economic espionage has never been a more significant issue than it is right now. Can you elaborate on this? Also in the article you stated that the Bay Area and Silicon Valley is a target-rich environment for espionage activity.

Are there certain areas of the country where the FBI and ICE find this activity to be pervasive? Or can we characterize this as pretty much a Nation-wide problem?

Mr. FIGLIUZZI. Mr. Chairman, with respect to your first question, as to whether this is increasing, whether it is more prevalent, whether it is on the increase, the answer is yes. The factors involve things like the global economic crisis.

What we are seeing—as I can talk about in this unclassified session—is that foreign nations and their intelligence services are understanding more than ever before that it is cheaper to steal our technology than to use their precious budget resources, in this time of global economic crisis, to research and develop it.

It is cheaper and it is faster to simply steal it. So we see nations, including in some cases some of our allies even willing, when it is in their economic interest, to steal intellectual property for their own economic benefits. With regard to your question about certain

areas of the country, there is no question that certain parts of our country have a bulls-eye on them.

Those would include areas like the research triangle in the Raleigh-Durham area of North Carolina; Silicon Valley in California; the Boston area, with a lot of research, cutting-edge research, going on there. But here is the risk in singling out areas. The risk in singling out specific areas is that it tends to put everybody at ease if they are not in those areas.

Our caseload shows that the real problem today is the unclassified-preclassified—what I call the Mom & Pop shop—research that is going on everywhere in this country, that is extremely vulnerable to targeting. We see them being targeted like never before.

Mr. LONG. Thank you.

With that, I would like to recognize Ranking Member Higgins for your questions.

Mr. HIGGINS. Thank you, Mr. Chairman.

Mr. Woods, according to your testimony the Immigration and Customs Enforcement leads the Government's efforts to prevent foreign adversaries from illegally obtaining U.S. military products and sensitive technology through its counterproliferation investigations unit. How does that unit work with other components, both within the Department of Homeland Security and outside of the agency, to identify potential vulnerabilities?

Could you go into as much detail as possible in an unclassified setting so that we can better understand the effectiveness of the collaborative efforts?

Mr. WOODS. Ah, yes. Thank you, Ranking Member Higgins.

ICE counterproliferation investigations works hand-in-hand with our partners in law enforcement, specifically the FBI and Department of Commerce. We also work with the Department of Defense Criminal Investigative Service on many cases involving military articles going overseas and going to the wrong hands.

I could say categorically this has been increasing over the last number of years, where we see our defense articles being routed to locations where they shouldn't be, through third countries. We combat this through several ways.

Most notably, we have a robust undercover operations program, where we engage the procurement networks that have been seeking these armaments and arms to go to these third countries. We use our undercover operations to move forward in investigating these sort of illicit procurement networks.

We also, in working with our partners, deconflict through the E2C2 to ensure that we are talking to the right people. We are making sure that we are not blue-on-blue. That we are making sure that if there is an effort by a state sponsor—we are working in close hands with the FBI to ensure that—that the sponsor is identified. Or whether it is an espionage type of case, that they are included in our investigation.

At the same note, if we identify a list of procurement networks that are going through to South America, we work on working with our partners overseas to ensure that we identify the networks that they are in source.

Mr. HIGGINS. Dr. Graham, according to your testimony the entire United States economy relies on some form of intellectual property.

You also stated that every two jobs in intellectual property-intensive industries support an additional one job elsewhere in the economy.

Given those numbers, can you explain to us the importance of protecting trade secrets in America, and can you further explain the true economic impact of espionage, economic espionage?

Mr. GRAHAM. Thank you, Mr. Higgins. Happy to comment on both those issues.

On the first issue, actually our report tends to undercount the employment impacts here. So while we found that there were on the order of 27 million American jobs in direct employment in these industries and 13 million in supply chain jobs, those are the upstream supply chain jobs—those jobs that were associated with those industries that were supplying into the IP-intensive industries.

There, of course, are other jobs in the downstream economy—distribution systems, retail systems—associated with these industries. So, you know, it really is a very large impact in the economy.

On the second question associated with the importance of trade secrecy protection, it is clear to us from everything we know—and many academic studies bear this out, surveys that have been done of American business managers, R&D managers at companies—that secrecy is among the most important protections that industries use to protect their innovations.

It tends to be much more effective than many of the other types of intellectual property. Of course, these different types of intentional property work together in very sophisticated and interesting ways because they complement one another. Trademarks will support, you know, a competitive advantage in marketing and sales, while the patents will protect the associated technological elements that go into the product.

So these things work together. But one thing that we fundamentally know is that secrecy is extremely important at maintaining competitive advantage. Which, of course, says something I mentioned earlier. It says something not only about what we have today—and the ability of the companies selling and engaging in business in the United States to sell and compete with those goods—but it also says something about the incentives to do innovation in the first place, right?

You know, we must be robust and focused on these issues. Because without that, of course, we tend to undermine the incentives of innovators that are looking for future profits in making a decision today to whether to do innovation.

So maintaining that important protection, and ensuring that the people at this table are doing the important work that they are doing is, of course, fundamental to supporting our system of innovation, which drives so much of the economic growth and the ability to give better lives to our people in the U.S. economy.

Mr. LONG. Thank you.

Thank you all for being here today and for your valuable testimony, and Ranking Member Higgins for his questions. The Members of the committee may have additional questions for the witnesses, and we will ask you all to respond to those in writing within 10 days for which the hearing will be open.

Without objection, the committee stands adjourned.
[Whereupon, at 10:55 a.m., the subcommittee was adjourned.]

○