AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

HOMELAND SECURITY INVESTIGATIONS: EXAMINING DHS'S EFFORTS TO PROTECT AMERICAN JOBS AND SECURE THE HOMELAND

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JULY 7, 2011

Serial No. 112–34

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

72–254 PDF WASHINGTON : 2012

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
MO BROOKS, Alabama

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
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
VACANCY

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

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT

MICHAEL T. MCCAUL, Texas, *Chairman*

GUS M. BILIRAKIS, Florida
BILLY LONG, Missouri, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

WILLIAM R. KEATING, Massachusetts
YVETTE D. CLARKE, New York
DANNY K. DAVIS, Illinois
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DR. R. NICK PALARINO, *Staff Director*
DIANA BERGWIN, *Subcommittee Clerk*
TAMLA SCOTT, *Minority Subcommittee Director*

CONTENTS

HOMELAND SECURITY INVESTIGATIONS: EXAMINING DHS'S EFFORTS TO PROTECT AMERICAN JOBS AND SECURE THE HOMELAND

Thursday, July 7, 2011

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 10:10 a.m., in Room 311, Cannon House Office Building, Hon. Michael T. McCaul [Chairman of the subcommittee] presiding.

Present: Representatives McCaul, Long, Duncan, and Thompson.

Also present: Representative Rogers.

Mr. MCCAUL. The committee will come to order. First order of business, I would like to ask for unanimous consent that the gentleman from Alabama Mr. Rogers, the Chair of the committee's Subcommittee on Transportation Security, be permitted to sit on the dais and participate in today's hearing. Without objection, so ordered.

This committee is meeting today to hear testimony from our private-sector working citizens in order to examine the effectiveness of DHS' enforcement policies and their impact on private industry, and I recognize myself now for an opening statement.

American innovation is the envy of the world. It is a constant target for competitors, including rogue nations that prefer to steal and copy rather than create. In addition to overcoming a depressed business climate, our Nation's job creators must protect their intellectual property from sophisticated counterfeiters all over the world, make sure their exports do not end up in the wrong hands, and comply with immigration laws. The consequences of failure are serious.

When counterfeit prescription drugs enter the marketplace or cheap imitation parts breach a semiconductor manufacturing plant, it costs American businesses revenues and jobs. When sensitive equipment manufactured for the Department of Defense falls into the wrong hands of rogue nations, it poses a threat to our National security. And when businesses seek assistance from the Government, it is the responsibility of the Department of Homeland Security to protect intellectual property, safeguard against counterfeit goods, maintain the integrity of export supply chains, and to en-

sure that businesses are in compliance with immigration laws in order to maintain a high-level playing field.

So today we ask these questions: Is the help they receive from DHS, in collaboration with other Government agencies, adequate? What improvements can be made? What more needs to be done? Indeed, several cases in recent years indicate that there is room for improvement in these measures that directly impact the bottom line of businesses and their ability to create jobs.

A 2008 investigation by Business Week magazine uncovered a polluted supply chain in some of our Nation's military equipment. According to Business Week, counterfeit products have been linked to the crash of mission-control networks, and they contain hidden back doors enabling network security to be bypassed and sensitive data accessed by hackers, thieves, and spies.

The same investigation found that as many as 15 percent of the spare parts and microchips the Pentagon buys are actually counterfeit. Recently, *Wired* magazine reported that the military purchased 59,000 counterfeit microchips from China in 2010. These chips were to be installed into an array of equipment, including U.S. missile-defense systems. This problem has been highlighted in many Federal prosecutions, including one in Houston where the defendant was sentenced to prison for selling counterfeit network cards to the U.S. Marine Corps for use in combat in Iraq and Afghanistan.

Pharmaceutical companies are seeing more of their products counterfeited. These counterfeits are often ineffective and, in some cases, dangerous. A recent report by CBS News found that the counterfeit drug network is worth an estimated $75 billion per year. This market has produced pharmaceutical drugs that contain little, none, or too much of the drug's active ingredient, and in some cases they contain harmful substances.

One recent case involved Mr. Ken Wang, the owner of a Houston-based company, who was convicted of conspiring with individuals in China to traffic in counterfeit and misbranded prescription drugs. ICE began its investigation after CBP seized 6,500 Viagra tablets from a mail facility in San Francisco addressed to Mr. Wang. Pfizer Pharmaceuticals, the manufacturer of Viagra, confirmed that these tablets were counterfeit and contained a substance used to manufacture sheetrock. I am sure some buyers were severely disappointed upon the receipt of these counterfeit Viagra. After being convicted, Mr. Wang fled to China, where he is still in hiding.

Such cases often involve a bizarre, multijurisdictional chain supply, making it difficult to prosecute and harder to track. In one instance the supply chain began with the medication being manufactured in mainland China, shipped to Hong Kong, then to the United Arab Emirates, and then, lastly, to the Bahamas. Once in the Bahamas, the individual prescriptions were filled, put into packets, addressed, and sent to the United Kingdom. From the United Kingdom, the drugs were then shipped to the consumers in the United States, who at the time believed—when they placed an order on-line believed they were purchasing them from a Canadian pharmacy.

ICE is the only Federal law enforcement entity with full statutory authority to pursue violations of U.S. export laws related to military items and controlled dual-use commodities, which will be another focus of this hearing. These are products that may have a seemingly innocuous civilian use, but also can have a potent military use as well.

A glaring example is the triggered spark gap. This device is used legally by doctors to break up kidney stones in patients; however, it can also be used to detonate a nuclear device. In one case, a Pakistani businessman with close ties to Pakistan military and linked to the militant Islamic groups attempted to use a third party in South Africa to purchase 200 triggered spark gaps. Under U.S. law, as a dual-use item, it is legal to export the devices to South Africa, but illegal to export them to Pakistan. The third-party buyer was arrested, but the Pakistani businessman has not yet been apprehended.

Finally, this subcommittee will examine the issue of worksite enforcement. In 2009, ICE, citing finite resources, instituted a shift in strategy from targeting undocumented employees to the employers that hire them. The results have been striking.

According to the Congressional Research Service, since 2008, administrative arrests have declined 77 percent, criminal arrests have declined 59 percent, and criminal convictions have declined 66 percent. These figures strongly suggest that the shift in strategy has led to a scaling back of worksite enforcement efforts that allow bad actors to get away with breaking the law with little or no penalty.

As is evident from my opening statement, ICE and CBP have a broad array of laws and issues they are responsible for enforcing, and we have a lot to talk about. I will, therefore, conclude my remarks by thanking our witnesses for being here today, and I do look forward to your testimonies.

[The information follows:]

PREPARED STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

The Committee on Homeland Security Subcommittee on Oversight, Investigations, and Management will come to order. The subcommittee is meeting today to hear testimony from our private sector witnesses in order to examine the effectiveness of DHS enforcement policies and their impact on private industry. I now recognize myself for an opening statement.

American innovation is the envy of the world. It is a constant target for competitors, including rogue nations that prefer to steal and copy rather than create.

In addition to overcoming a depressed business climate, our Nation's job creators must protect their intellectual property from sophisticated counterfeiters all over the world, make sure their exports do not end up in the wrong hands, and comply with immigration laws.

The consequences of failure are serious. When counterfeit prescription drugs enter the marketplace or cheap imitation parts breach a semiconductor manufacturing plant it costs American businesses revenue and jobs. When sensitive equipment manufactured for the Department of Defense falls into the hands of rogue nations, it poses a threat to our National security.

When businesses seek assistance from the Government, it is the responsibility of the Department of Homeland Security to protect intellectual property, safeguard against counterfeit goods, maintain the integrity of export supply chains and to ensure that businesses are in compliance with immigration laws in order to maintain a level playing field.

Today we ask: Is the help they receive from DHS, in collaboration with other Government agencies, adequate? What improvements can be made? And what more can be done? Indeed, several cases in recent years indicate that there is room to improve

these measures that directly impact the bottom line of businesses and their ability to create jobs.

A 2008 investigation by *Businessweek* magazine uncovered a polluted supply chain in some of our Nation's military equipment. According to Businessweek: "Counterfeit products have been linked to the crash of mission-critical networks, and may contain hidden 'back doors' enabling network security to be bypassed and sensitive data accessed by hackers, thieves, and spies." The same investigation found that as many as 15% of the spare parts and microchips the Pentagon buys are counterfeit.

Recently *Wired* Magazine reported that the military purchased 59,000 counterfeit microchips from China in 2010. These chips were to be installed into an array of equipment, including U.S. missile defense systems.

This problem has been highlighted in many Federal prosecutions, including one in Houston where the defendant was sentenced to Federal prison for selling counterfeit network cards to the U.S. Marine Corps for use in combat in Iraq and Afghanistan.

Pharmaceutical companies are seeing more of their products counterfeited. These counterfeits are often ineffective and, in some cases dangerous. A recent report by CBS News found that the counterfeit drug network is worth an estimated $75 billion dollars per year. This market has produced pharmaceutical drugs that contain little, none, or too much of the drug's active ingredients. In some cases, the drugs contained harmful substances.

One recent case involved Mr. Ken Wang, the owner of a Houston-based company, who was convicted of conspiring with individuals in China to traffic in counterfeit and misbranded prescription drugs. ICE began its investigation after CBP seized 6,500 loose Viagra tablets from a mail facility in San Francisco addressed to Mr. Wang. Pfizer Pharmaceuticals, the manufacturer of Viagra, confirmed that the tablets were counterfeit and contained a substance used to manufacture sheetrock. After being convicted, Mr. Wang fled to China, where he is still in hiding.

Such cases often involve a bizarre, multijurisdictional supply chain, making it difficult to prosecute and harder to track. In one instance, the supply chain began with the medication being manufactured in mainland China, shipped to Hong Kong, then the United Arab Emirates and lastly to the Bahamas. Once in the Bahamas, the individual prescriptions were filled, put into packets, addressed, and sent to the United Kingdom. From the United Kingdom the drugs were shipped to the consumer in the United States who, at the time of placing their on-line order, believed they were purchasing them from a Canadian pharmacy.

ICE is the only Federal law enforcement entity with full statutory authority to pursue violations of U.S. export laws related to military items and controlled dual-use commodities. These are products that may have a seemingly innocuous civilian use, but also can have a potent military use as well. A glaring example is the triggered spark gap. This device is used legally by doctors to break up kidney stones in patients. However, it can also be used to detonate a nuclear device.

In one case, a Pakistani businessman with close ties to the Pakistani military, and linked to militant Islamic groups, attempted to use a third-party in South Africa to purchase 200 triggered spark gaps. Under U.S. law, as a duel-use item, it is legal to export the devices to South Africa, but illegal to export them to Pakistan. The third-party buyer was arrested, but the Pakistani businessman has not yet been apprehended.

Finally, the subcommittee will examine the issue of worksite enforcement.

In 2009, ICE, citing "finite resources", instituted a shift in strategy from targeting undocumented employees to the employers that hire them.

The results have been striking. According to the Congressional Research Service, since 2008, administrative arrests have declined 77 percent, criminal arrests have declined 59 percent, and criminal convictions have declined 66 percent.

These figures strongly suggest that this shift in strategy has lead to a scaling back of worksite enforcement efforts that allow bad actors to get away with breaking the law with little or no penalty.

As is evident from my opening statement, ICE and CBP have a broad array of laws and issues they are responsible for enforcing and we clearly have much to talk about today. I will therefore conclude my remarks by thanking our witnesses for being here. I look forward to each of your testimonies.

Mr. MCCAUL. I see that my Ranking Member of the subcommittee Mr. Keating is not available today. I believe he is attending a funeral back in his district, and with that, I will recog-

nize the Ranking Member of the full committee, the gentleman from Mississippi, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Mr. Chairman, for convening this hearing.

We are here today to discuss the work of the Homeland Security Investigations Division of ICE, responsible for a wide range of duties from investigations involving the illegal production, smuggling, and distribution of counterfeit and priority products to money laundering violations and workplace immigration enforcement efforts. ICE Homeland Security Investigation is called upon to handle these matters on very stretched resources.

ICE Homeland Security Investigation's International Affairs Unit also represents the largest investigative law enforcement presence abroad from the Department of Homeland Security, yet, according to ICE and the Intellectual Property Enforcement Coordinator, they are required to do much with very little.

In this Congress, the majority passed H.R. 1, which cut $350 million from the Department of Homeland Security budget for border security and technology. Despite these financial and staffing changes, the Obama administration has made numerous advances in confronting both worksite enforcement and intellectual property issues.

For example, Operation Network Raider, a collaborative interagency initiative aimed at ending illegal distribution of counterfeit network hardware manufacturing in China, resulted in 30 felony convictions and over 700 seizures of counterfeit hardware valued at more than $143 million. In fiscal 2010, ICE intellectual property investigations are up more than 41 percent, arrests are up more than 37 percent, and the Department of Homeland Security intellectual property seizures are up more than 34 percent.

Regarding worksite enforcement, in April 2009, the administration shifted the country's focus from large-scale raids, which cost millions and yielded minimal criminal convictions, to focusing on unscrupulous employers that hire and sometimes exploit undocumented immigrants. Prior to this shift in strategy, ICE conducted numerous high-profile worksite raids that were high on costs, but low on substance.

In August 2008, one of the largest raids occurred in Laurel, Mississippi, where over 600 workers were detained. Approximately 475 of the 600 workers were detained; yet, according to reports, only 8 appeared in Federal court to face criminal charges. This form of military-style raids destroyed families, disrupted local economies, and had a negative impact on small towns and rural communities.

The new approach represents an aggressive enforcement strategy that targets the worst employers. A major focus of this strategy is the audit of Form I–9, Employment Eligibility Verification Form. ICE use of Form I–9 audits to test an employer's compliance with existing documentation laws has skyrocketed from 254 in fiscal year 2007 to 2,196 in fiscal year 2010. Furthermore, forced removals are at a record high, 393,000 in fiscal year 2009, up from 30,000 in fiscal year 1990; as well as detentions, which are at a record high of over 360,000 in fiscal year 2010, up from 95,000 in fiscal year 2001.

But let me be clear, enforcement alone will not fix our immigration system. Congress can no longer delay enacting comprehensive immigration reform and should immediately do what the American people demand: Fix the broken immigration system, not enact more piecemeal policies that don't solve the problem.

I am looking forward to receiving the testimony of our private-sector witnesses; however, I know that it is ultimately the responsibility of multiple Federal partners to enforce our immigration laws and prevent counterfeit goods from entering into our supply chain. ICE, CBP, FDA, and the newly created Intellectual Property Enforcement Coordinator could have provided helpful testimony on existing challenges and recommendations for staying ahead of changes in technology that make intellectual property theft a constantly moving target. Furthermore, testimony from ICE would have revealed the strides that have been made under the country's new worksite enforcement approach. Unfortunately, they were not invited to testify, and as a result, the record will not reflect the facts that they could have provided.

However, I do look forward to the testimony, Mr. Chairman, as I indicated, and I yield back the balance of my time.

Mr. MCCAUL. I thank the Ranking Member, and other Members may submit opening statements for the record.

[The statement of Hon. Bilirakis follows:]

PREPARED STATEMENT OF HONORABLE GUS M. BILIRAKIS

JULY 7, 2011

Thank you, Mr. Chairman, and thank you for holding this important hearing.

The American economy has been working for the last several years to climb out of its economic rut. In my Congressional district in the Tampa Bay area, and throughout the State of Florida, the unemployment rate is still in double digits, which is far too high. I regularly visit with businesses throughout my Congressional district. Too often, I hear from them that the Federal Government appears, at best, indifferent to the concerns of America's job creators.

In the global marketplace that we live and work in, we must ensure that sensitive products and services do not end up in the hands of those who wish to harm us, while at the same time allowing American employers and employees to compete with the rest of the world and create much-needed jobs. Entities within the Department of Homeland Security are tasked with enforcing our laws pertaining to intellectual property rights, commercial fraud, export control, and worksite immigration enforcement. We must ensure that Immigrations and Customs Enforcement (ICE) and Customs and Border Protection (CBP) are working seamlessly with the private sector in the most effective and efficient ways possible to prohibit pirated goods from entering our marketplace, counterfeit medicines from harming our sick, jobs from going to illegal immigrants, and sensitive security technology from falling in the hands of our enemies.

These goals can best be achieved through a cooperative and collaborative approach, rather than an adversarial relationship with American businesses. I look forward to learning how the Congress and the Department can work together with the private sector to help ensure that our economic strength and freedoms and National security are not compromised.

I yield back.

Mr. MCCAUL. Before I introduce the witnesses, I ask unanimous consent to insert into the record statements from the Motion Picture Association of America and the Recording Industry Association of America. Without objection, so ordered.

[The information follows:]

STATEMENT OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.

JULY 7, 2011

A. BACKGROUND AND INTRODUCTION

We want to thank the subcommittee for holding this oversight hearing to review the efforts of the Department of Homeland Security to combat counterfeiting, trademark, and intellectual property theft, a crime that damages our economy and threatens American jobs. We appreciate the opportunity to submit this statement on behalf of the Motion Picture Association of America, Inc.[1] and its member companies regarding the serious and growing threat of this crime. As the primary voice and advocate for the American motion picture, home video, and television industries in the United States and around the world, we have witnessed the proliferation of web-based enterprises dedicated solely to stealing the product of our industry's workforce and are gravely concerned about the detrimental impact that digital theft has on the millions of American men and women who work in our industry.

The U.S. intellectual property (IP) industries—of which ours is one—are critical to the health of our economy. Our industry alone produces billions in tax revenue each year, consistently generates a positive balance of trade with every country in the world, and has shown it can contribute to the economic recovery of areas hard-hit by the recession. We are woven into the fabric of the U.S. economy.

More than 2.4 million working Americans residing in all 50 U.S. States rely on the motion picture and television industry for their livelihoods. While it is true that our industry employs some well-known artists, that is not the real story of our business. Whether they are set builders, costume designers, electricians, assistant directors, or cast members, the overwhelming majority of those who work behind the scenes in our industry are middle-class workers who are proud to be part of a business that has created a quintessential American product for almost 100 years: filmed entertainment. The major motion picture companies represent only a fraction of the businesses that make up our industry, as there are a host of U.S. companies who play a critical role in the creation of filmed entertainment providing technologies and services utilized in every step of the post-production process. More than 95,000 small businesses—93 percent of whom employ fewer than 10 people—are involved in the production and distribution of movies and television. Those individuals, small business owners and their families are extremely vulnerable to changes in the production economy.

We appreciate the efforts of the Immigration and Customs Enforcement (ICE) agency to combat digital theft and counterfeiting for a range of U.S. industries. In the case of the entertainment industry, the theft of motion picture and television productions threatens the economic vitality of our business, and the millions of American working men, women, and local small businesses that depend on it. The websites targeted by ICE—via a transparent process that requires a judicial finding of probable cause—are not "innocent" internet users; they are illegal for-profit businesses knowingly trafficking in stolen and counterfeit goods. They pose a threat to us, to movie theaters large and small, to the American public who unknowingly gives over personal financial income to unscrupulous traders, and to the health of the U.S. economy. In the past decade, we have seen increasing evidence that organized crime and terrorist organizations are engaging in counterfeiting and intellectual property theft to support a variety of criminal activities.[2] ICE, by initiating Operation In Our Sites in June 2010, has stepped forward to protect U.S. industries and citizens from this form of cybercrime.

Digital theft threatens the jobs of all who work in our business. Such theft destroys the ability of those who finance and produce filmed entertainment to recoup their investment, and in turn, the ability of film artists to continue to create. The majority of films produced must secure financing and distribution partners prior to production. Digital theft damages the confidence of those partners in their ability to do so, the end result being a diminished number of films being made and American jobs disappearing.

We are not talking about a distant future. Over the last 3 months, no fewer than three reports have demonstrated that infringing content represents a significant

[1] The Motion Picture Association of America and its international counterpart, the Motion Picture Association (MPA) serve as the voice and advocate of the American motion picture, home video, and television industries, domestically through the MPAA and internationally through the MPA. MPAA members are Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, Walt Disney Studios Motion Pictures, and Warner Bros. Entertainment Inc.

[2] "Film Piracy, Organized Crime, and Terrorism" Published 2009 by the RAND Corporation.

percentage of global internet traffic. Most recently, a report released by Envisional, an independent internet consulting company, estimated that almost a quarter of global internet traffic and over 17 percent of U.S. internet traffic is copyright infringing. This is a level of theft that cannot be sustained without significant damage to the motion picture industry, the workforce it supports, and the American economy.

The Intellectual Property Enforcement Coordinator's (IPEC) Joint Strategic Plan on Intellectual Property Enforcement released in June 2010 committed to using these resources and existing resources to increase law enforcement activity. ICE, the Department of Justice, and the IPR Center have stepped forward to carry out that mandate. Operation In Our Sites has not only put illegal sites out of business, but has raised public awareness about this specific form of crime on the internet. Most importantly, these enforcement efforts have resulted in most of these entities ceasing their illegal activity. Movies and TV programs, some of the biggest draws on the internet, are in many ways the "canary in the coal mine." Stealing and illegally selling this content may appear to be victimless crimes or a harmless form of theft, but they are neither. If it is not made clear that this kind of activity is illegal, it has the potential to become the harbinger of even more forms of illegal activity on the internet.

Again, we appreciate the opportunity to submit this statement and applaud the subcommittee for holding this important oversight hearing. We look forward to working with Congress to support strong IP enforcement and to secure the additional resources that will protect our industry—and American jobs—from those who engage in the illegal activity of digital theft with disregard.

LETTER FROM THE RECORDING INDUSTRY ASSOCIATION OF AMERICA

JULY 7, 2011.

The Honorable MICHAEL T. MCCAUL,
Chairman, Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, 131 Cannon House Office Building, Washington, DC 20515.

DEAR CHAIRMAN MCCAUL: On behalf of the RIAA[1] and its member companies, I want to thank you for holding today's hearing examining the work of the Department of Homeland Security to protect American jobs. I believe it is important to recognize the significant anti-piracy work of the U.S. Immigration and Customs Enforcement Bureau. ICE's considerable enforcement efforts have been invaluable in protecting our industry's—and our country's—valuable creative works.

In particular, I would like to bring attention to ICE's on-going program, Operation In Our Sites. This initiative has brought much-needed attention to the rogue online sites dedicated to infringement of copyrighted and trademarked works, and takes appropriate and necessary action to stop their illegal activity. These illicit businesses have, until recently, operated with near-impunity, making millions of dollars through the theft and unauthorized distribution of others' products and content. The result has been the loss of thousands of jobs, of billions in economic development, and of countless creators who can't afford to make new contributions to our culture and economy.

We understand how easy it is, particularly in the digital era, to wave off the value of recorded music. Yet, our industry contributes billions to our economy and remains one of our country's most important exports. And few can deny the importance of music in our everyday lives. Keeping the U.S. music industry the envy of the world requires increased vigilance and action. We greatly appreciate ICE for recognizing the growing threats to these works on-line, and for taking the necessary steps to ensure they are properly protected. We look forward to working with the Committee on Homeland Security, the Department and other interested parties in the future.

Sincerely,

MITCH BAINWOL,
Chairman and CEO.

Mr. MCCAUL. Mr. Brian Toohey is the president of Semiconductor Industry Association and has served in this capacity since 2010. His responsibilities include crafting and leading SIA's policy

[1] The Recording Industry Association of America, Inc. ("RIAA") is a trade association whose member companies create, manufacture, and/or distribute approximately 85% of all legitimate sound recordings produced and sold in the United States.

agenda and serving as an advocate for U.S. semiconductor design and manufacturing across the globe. Prior to joining SIA, Mr. Toohey served in leadership positions at the Pharmaceutical Research and Manufacturers of America, DKA Research and Development, and the Europe office of the U.S. Department of Commerce. He holds an undergrad and graduate degree from Georgetown University School of Foreign Service, and he currently serves as an adjunct professor. Welcome here today.

Mr. Michael Russo is the global security director for Eli Lilly and Company. Mr. Russo is responsible for the management of Lilly's global product protection security team, which includes eight experienced investigators based in Asia, Europe, and the United States. His team handles cases involving counterfeit, stolen, and diverted pharmaceuticals. Mr. Russo joined Eli Lilly in 1997 as a global security associate and has supported various security roles prior to his current assignment. He is a native of Indianapolis and received a bachelor of science in public administration and criminal justice from Indiana University; also a graduate of the FBI National Academy at Quantico, Virginia; and the United States Secretary Service Dignitary Protection School. Welcome, Mr. Russo.

Next we have Mr. Mario Mancuso, who is a corporate partner at the Fried Frank in Washington, DC. He is a leading authority on U.S. regulation and international trade and export control enforcement. From 2007 to 2009, he served as Under Secretary for Industry and Security at the U.S. Department of Commerce. In this role Mr. Mancuso was responsible for, among many other things, identifying and opening key export markets around the world for U.S. technology products consistent with the United States' security interests. He graduated magna cum laude from Harvard University and received his law degree from the New York University School of Law; former Army infantry officer. He is a combat veteran of Operation Iraqi Freedom, and we thank you for that.

Ms. Jana Baker McNeill is a senior policy analyst for homeland security at The Heritage Foundation. Today Ms. McNeill is testifying as a private citizen. She is an expert on homeland security and science and technology issues, including the issue of worksite enforcement of immigration laws. She has provided commentary in her research and writings on multiple media outlets and renowned publications. Before joining Heritage, she worked as a research assistant for the Hutchinson Group; also worked as an environmental management consultant for Booz, Allen, Hamilton. Prior to that, she worked on the staff of Maryland Governor Robert Ehrlich. Ms. McNeill graduated from the University of Arkansas Little Rock School of Law and has a bachelor's degree in environmental science from the University of Maryland.

With that, I want to thank the witnesses for being here today. I think this will be very interesting testimony, and now the Chair recognizes Mr. Brian Toohey for his remarks.

STATEMENT OF BRIAN TOOHEY, PRESIDENT, SEMICONDUCTOR INDUSTRY ASSOCIATION

Mr. TOOHEY. Thank you, Chairman McCaul, Ranking Member Thompson, and the other Members of the subcommittee. Greatly appreciate the opportunity to be here today before this oversight

subcommittee to testify about the dangers that counterfeit semiconductors pose to U.S. National security and public safety, as well as the proven, common-sense steps that DHS can take to prevent counterfeit chips from entering military and civilian supply chains.

This issue is of more and more importance as semiconductors are being used in an increasing number of mission-critical applications such as life-saving medical devices, automotive safety systems, airplanes, and military equipment.

By way of brief background, the semiconductor industry is America's largest export industry. Semiconductor innovations form the foundation of America's trillion-dollar technology industry that supports a workforce of nearly 6 million in the United States. The semiconductor industry is a great American innovation story invented here, and our companies still lead the world in the pace of innovation and global market share, and we consider our industry a model for the innovation economy of the future. Our companies still do the vast majority of advanced design and manufacturing here in the United States and sell nearly 85 percent of our products internationally.

But the importation of counterfeit semiconductor chips is a growing National security and health and safety threat. For years manufacturers abroad, primarily in China, have used crude techniques, including surface sanding, acid washes, and other procedures, to turn e-waste into counterfeit semiconductors. These chips, already weakened from their original state and at great risk of failure, are then relabeled using digital printing and laser-etching techniques, and packaged for sale to international brokers.

Recently counterfeiters have begun acquiring even more sophisticated equipment and advanced techniques, making it increasingly difficult to identify fake semiconductors. As a result, more and more counterfeit chips make it through our borders into a wide range of products, including automobile technology, such as brake systems; health care technology, such as defibrillators; and, most troubling, into military equipment, such as missiles, navigation systems, and jets. Given their high risk of failure, this places our citizens and our military personnel at unreasonable risk.

I would like to draw the subcommittee's attention to Exhibit No. 1 up on the screen. This is a picture of an authentic and counterfeit voltage regulator for an automotive air bag and braking system. Very, very difficult to tell the difference between the two, and I will explain more about the markings in my testimony.

Experts have estimated that 15 percent of all spare and replacement semiconductors purchased by the Pentagon are counterfeit, and DHS is equally vulnerable. Overall, more than $7 billion of counterfeit chips are sold in the United States every year. Our industry takes this threat very seriously and is committed to doing everything within our power from establishing publicly available databases of authorized distributors to training Customs officials around the world to working cooperatively with U.S. law enforcement.

We appreciate the Obama administration's commitment to intellectual property rights and its resolve to prevent counterfeit goods from entering our borders. U.S. Immigration and Customs Enforcement, the Federal Bureau of Investigation, the Department of Jus-

tice, and Department of Defense all play crucial roles in combating the infiltration of counterfeit goods, including semiconductors, and we have been working cooperatively with these agencies for many years.

Historically, Customs and Border Protection also facilitated anticounterfeiting efforts. Prior to 2000, when port officers suspected a shipment contained counterfeit chips, they would contact the manufacturer and share one of the products. After 2000, but before 2008, port officers photographed the outside of suspected chips and sent the publicly viewable information to the chip manufacturer whose trademark appeared on the surface to determine whether the chip was counterfeit. Using highly confidential databases, manufacturers then determined very quickly, in about 85 percent of the cases, whether or not the chips were counterfeit by analyzing the codes on the surface of the chip. It was a system that worked very well and prevented enormous quantities of counterfeit chips from entering the United States.

In mid-2008, however, CBP officers were instructed to redact or cross out the identifying marks in the photographs except the trademarks before sending them to manufacturers, thereby scuttling the cooperative system that worked so well for so many years. The current redaction practice makes it virtually impossible for the industry, much less the importer or CBP, to authenticate suspected counterfeit semiconductors. U.S. Treasury officials argue that this policy shift is intended to shield port officers from criminal liability for disclosure of confidential information; however, to the extent the codes on the surface of semiconductors which are publicly viewable to anyone who picks up the chip or looks at the label are confidential, they belong to the manufacturers to whom the photographs would be sent.

We respectfully ask this subcommittee to exercise its oversight authority to insist that CBP revert to its historical practice of sharing the unredacted photographs and, where necessary, the physical products of suspected counterfeit semiconductors with manufacturers. Such a policy is clearly in the National interest and public safety. It is a practical, discrete action that could be implemented today. It would stop untold number of counterfeits at our borders, improve our National security, and save American lives.

Thank you for this opportunity. I would welcome any questions.

[The statement of Mr. Toohey follows:]

PREPARED STATEMENT OF BRIAN TOOHEY

EXECUTIVE SUMMARY

The importation of counterfeit semiconductor "chips" is a growing National security threat. For years, manufacturers abroad (primarily in China) have used crude techniques, including open fires, surface sanding, and acid washes, to turn "e-waste" into counterfeit semiconductors. These chips—already weakened from their original state and at great risk of failure—are then re-labeled using digital printing and laser etching and packaged for sale to international brokers. However, counterfeiters have begun acquiring more sophisticated equipment and advanced counterfeiting techniques, making it increasingly difficult to identify counterfeit semiconductors. As a result, more and more counterfeit chips make it through our borders and into a wide range of products, including automobile technology such as brake systems, health care technology such as defibrillators, and, most troublingly, into military equipment such as missiles, navigation systems, and jets. Given their high-failure

risk, counterfeit infiltration places our citizens and military personnel in unreasonable peril.

SIA appreciates the Obama administration's commitment to intellectual property rights and its resolve to prevent counterfeit goods from entering the United States supply chain. Immigrations and Customs Enforcement ("ICE"), the Federal Bureau of Investigation ("FBI"), the Department of Justice ("DOJ"), and the Department of Defense ("DOD") have all played crucial roles in combating the infiltration of counterfeit goods.

Historically, Customs and Border Protection (CBP) has also facilitated anti-counterfeiting efforts. Prior to 2000 when Port Officers suspected a shipment contained counterfeit chips, they would contact the trademark owner and share one of the products. After 2000 but before 2008, Port Officers photographed the outside of a suspect chip and sent the publicly viewable information to the chip manufacturer whose trademark appeared on the surface of the chip to determine whether the chip was counterfeit. Using a highly confidential database, the trademark owner could then determine very quickly, in almost 85% of the requests, whether or not the chips were counterfeits by analyzing the codes on the surface of the chip.

In mid-2008, however, CBP Officers were instructed to redact any identifying marks in the photographs, except the trademark, before sending them to manufacturers, thereby scuttling the cooperative system that worked so well for 8 years. The current redaction practice makes it impossible for the industry, much less the importer or CBP, to authenticate suspected counterfeit semiconductors. U.S. Treasury officials argue that its policy shift is intended to shield Port Officers from criminal liability for the disclosure of confidential information. However, to the extent the codes on the surface of semiconductors, which are publicly viewable to anybody who picks up a chip or looks at a chip's packaging label, are confidential, they belong to the manufacturers to whom photographs would be sent.

SIA simply asks CBP to revert to its historical pre-2008 practice and share unredacted photographs, and where necessary physical products, of suspected counterfeit semiconductors with semiconductor manufacturers. Such a policy is clearly in the Nation's National security interest. Preventing counterfeit semiconductors from entering the United States will protect public safety and safeguard the military supply chain.

Chairman McCaul, Ranking Member Keating, and other Members of the subcommittee, my name is Brian Toohey. I am the President of SIA, the Semiconductor Industry Association ("SIA"). I thank the committee for inviting me to testify about the dangers that counterfeit semiconductors pose to the U.S. military and the civilian population at large, as well as the common-sense steps the Obama administration can take to prevent counterfeit semiconductors from entering highly sensitive military and civilian supply chains. This issue is more and more important as semiconductors are being used in an increasing number of mission-critical applications such as medical lifesaving equipment, car brakes and air bag systems, nuclear reactors, airplanes and military weapon systems.

SIA is the voice of the U.S. semiconductor industry, America's largest export industry since 2005 and a bellwether of the U.S. economy. Semiconductor innovations form the foundation for America's $1.1 trillion dollar technology industry affecting a U.S. workforce of nearly 6 million. Founded in 1977 by five microelectronics pioneers, SIA unites more than 60 companies from across the United States that account for 80 percent of the Nation's semiconductor production. Our industry has an especially robust presence in Texas and Massachusetts, with SIA members AMD, Freescale, Intel, STMicroelectronics and Texas Instruments in Texas, and Analog Devices, Intel, Maxim and Rochester Electronics in Massachusetts. SIA seeks to strengthen U.S. leadership in semiconductor design and manufacture by working with Congress, the administration, and other industry groups to enable the right ecosystem for technology development and commercialization. Specifically, SIA encourages policies and regulations that fuel innovation, propel business and drive international competition in order to maintain a thriving semiconductor industry in the United States.

BACKGROUND ON SEMICONDUCTORS

Semiconductor "chips" are used in everything that is computerized or uses radio waves. Indeed, semiconductors are components in a staggering variety of products, from computers and smart phones to medical devices, LEDs and smart meters, automobiles and military equipment, including missiles, navigation systems and jets. They are making the world around us smarter, greener, safer, and more efficient. They are also economically vital to the Nation. In 2010, U.S. semiconductor companies generated over $140 billion in sales—representing nearly half the worldwide

market, and making semiconductors the Nation's largest export industry. Our industry directly employs nearly 200,000 workers in the United States, and another 6 million American jobs are made possible by the use of semiconductors. Studies show that semiconductors, and the information technologies they enable, represent 3 percent of the economy, but drive 25 percent of economic growth.

INCREASING PREVALENCE OF COUNTERFEITS

Due to the increasing availability and decreasing price of equipment needed to counterfeit semiconductors, unscrupulous brokers looking to garner illicit profits are importing ever greater numbers of counterfeit chips into the United States. In fact, the Department of Commerce has reported that counterfeit incidents discovered by the military and military suppliers more than doubled between 2005 and 2008, from 3,868 to more than 9,356 cases.[1] Alarmingly, these counterfeit chips can be found in automobile airbag systems, defibrillators, and even highly sensitive military equipment. As *BusinessWeek* explains:

"The American military faces a growing threat of potentially fatal equipment failure—and even foreign espionage—because of counterfeit computer components used in warplanes, ships, and communications networks. Fake microchips flow from unruly bazaars in rural China to dubious kitchen-table brokers in the U.S. and into complex weapons. Senior Pentagon officials publicly play down the danger, but government documents, as well as interviews with insiders, suggest possible connections between phony parts and breakdowns. In November 2005, a confidential Pentagon-industry program that tracks counterfeits issued an alert that 'BAE Systems experienced field failures,' meaning military equipment malfunctions, which the large defense contractor traced to fake microchips . . . In a separate incident last January, a chip falsely identified as having made by Xicor . . . was discovered in the flight computer of an F–15 fighter jet at Robins Air Force Base . . . Special Agent Terry Mosher of the Air Force Office of Special Investigations confirms that the 409th Supply Chain Management Squadron eventually found four counterfeit Xicor chips."[2]

Some experts have estimated that as many as 15 percent of all spare and replacement semiconductors purchased by the Pentagon are counterfeit.[3]

Many counterfeit chips are traced back to China. *BusinessWeek* writers visited China and described the counterfeiting economy as follows:

"The traders typically obtain supplies from recycled-chip emporiums such as the Guiyu Electronics Market outside the city of Shantou in southeastern China. The garbage-strewn streets of Guiyu reek of burning plastic as workers in back rooms and open yards strip chips from old PC circuit boards. The components, typically less than an inch long, are cleaned in the nearby Lianjiang River and then sold from the cramped premises of businesses such as Jinlong Electronics Trade Center. A sign for Jinlong Electronics advertises in Chinese that it sells 'military' circuitry, meaning chips that are more durable than commercial components and able to function at extreme temperatures. But proprietor Lu Weilong admits that his wares are counterfeit. His employees sand off the markings on used commercial chips and relabel them as military. Everyone in Guiyu does this, he says: 'The dates [on the chips] are 100% fake, because the products pulled off the computer boards are from the '80s and '90s, [while] consumers demand products from after 2000.'[4]

While the Chinese have admitted the prevalence of semiconductor counterfeiting in China, Chinese officials claim they can do little about the counterfeiting. As Wayne Chao, secretary general of the China Electronics Publishing Association and

---

[1] U.S. Department of Commerce, Defense Industrial Base Assessment: Counterfeit Electronics available at *http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf;* see also Michele Moss, *Systems Assurance, The Global Supply Chain, and Efforts to Increase Communication Between Acquisition and Development,* available at *http://www.dtic.mil/ndia/2010CMMI/WednesdayTrack4_11328Moss.pdf; Surge in counterfeit items in Pentagon's supplies,* Homeland Security Newswire, Aug. 10, 2010, available at *http://www.homelandsecuritynewswire.com/surge-counterfeit-items-pentagons-supplies.*

[2] Brian Grow et al., *Dangerous Fakes: How counterfeit, defective computer components from China are getting into U.S. warplanes and ships,* BusinessWeek, Oct. 2, 2008, available at *http://www.businessweek.com/magazine/content/08_41/b4103034193886.htm.*

[3] Id.

[4] Id.

anticounterfeiting advocate said, "[e]veryone wants to blame China. But it's difficult to differentiate between a legitimate product and a fake."[5]

ADMINISTRATION RESOLVE TO COMBAT COUNTERFEITS

Mr. Chao is correct—it is difficult to differentiate between a legitimate semiconductor and a fake. And it is precisely because of the difficulties inherent in differentiating between a legitimate and counterfeit semiconductor that the Government must place a single-minded emphasis on preventing the importation of counterfeit chips.[6] Thankfully, the Obama administration—like the previous Bush and Clinton administrations—has shown an admirable resolve to combat counterfeiting and other forms of intellectual property theft. Indeed, President Obama himself has promised:

"We're going to aggressively protect our intellectual property. Our single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century."[7]

Last year, DOJ, ICE, the Office of Homeland Security Investigations, Naval Criminal Investigative Service ("NCIS"), Postal Inspection Service, Internal Revenue Service, Department of Transportation, and General Services Administration worked together with the semiconductor industry on an investigation that led to the indictments of the principals of a Florida-based company that generated nearly $16 million in gross receipts between 2007 and 2009 by importing nearly 60,000 counterfeit semiconductors from China and selling them to the military as "military grade."[8] As the U.S. Attorney in charge of the investigation explained:

"Product counterfeiting, particularly of the sophisticated kind of equipment used by our armed forces, puts lives and property at risk. This case shows our determination to work in coordination with our law enforcement partners and the private sector to aggressively prosecute those who traffic in counterfeit parts."

The Obama administration's Intellectual Property Enforcement Coordinator, Victoria Espinel, also understands the importance of enforcing intellectual property laws and preventing the importation of counterfeit semiconductors. In the administration's 2010 Joint Strategic Plan on Intellectual Property Enforcement, Ms. Espinel explained the vital role of intellectual property enforcement in protecting the consumer safety and National security:

"Violations of intellectual property rights, ambiguities in law and lack of enforcement create uncertainty in the marketplace, in the legal system and undermine consumer trust. Supply chains become polluted with counterfeit goods. Consumers are uncertain about what types of behavior are appropriate and whether the goods they are buying are legal and safe. Counterfeit products can pose a significant risk to public health, such as . . . military systems with untested and ineffective components to protect U.S. and allied soldiers, auto parts of unknown quality that play critical roles in securing passengers and suspect semiconductors used in life-saving defibrillators . . . Intellectual property infringement [also] can undermine our national and economic security. This includes counterfeit products entering the supply chain of the U.S. military, and economic espionage and theft of trade secrets by foreign citizens and companies."[9]

Unfortunately, despite the Obama administration's understanding of the dangers posed by counterfeit semiconductors, a 2008 Customs and Border Protection ("CBP") action required by the Department of the Treasury is frustrating the efforts of other Government agencies to combat the importation of counterfeit chips.

---

[5] Id.

[6] See Exhibit 1, a photograph comparing a genuine and counterfeit semiconductor.

[7] Victoria Espinel, 2010 Joint Strategic Plan on Intellectual Property Enforcement 3, available at *http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf* ("IPEC Report").

[8] Press Release, U.S. Department of Justice, *Owner and Employee of Florida-based Company Indicted in Connection with Sales of Counterfeit High Tech Devices Destined to the U.S. Military and Other Industries* (Sept. 14, 2010), available at *http://www.justice.gov/criminal/cybercrime/wrenIndict.pdf;* Spencer H. Hsu, *U.S. charges Florida pair with selling counterfeit computer chips from China to the U.S. Navy and military,* Washington Post, Sept. 14, 2010, available at *http://www.washingtonpost.com/wp-dyn/content/article/2010/09/14/AR2010091406468.html.*

[9] IPEC Report at 4.

CBP ACTION HALTS INDUSTRY ASSISTANCE IN COMBATTING COUNTERFEITING

Historically, when a CBP Port Officer suspected that an imported semiconductor was counterfeit, CBP would send the manufacturer of the semiconductor (as identified by the trademarks featured on the semiconductor) either a sample of a suspect semiconductor or a photograph of the surface of the suspect chip. The surface of semiconductors contain identifying manufacturing marks—these usually represent part number, lot number, date of manufacture and place of manufacture—all in clear sight to anyone looking at the chip. The meaning of these identifying marks, however, is known only to the manufacturer—and only the manufacturer of the semiconductor can identify the authenticity of the chip using highly confidential and proprietary company-specific databases. After receiving a photograph of a suspected counterfeit chip, a semiconductor manufacturer would quickly locate the specific product in its internal computer systems, determine the product's authenticity, and inform CBP of its determination. CBP could then seize the counterfeit chips. While this policy did not prevent all counterfeits from entering the country, it did lead to numerous successful raids of counterfeit manufacturers in China and brokers in the United States.[10]

Unfortunately, in August 2008 manufacturers discovered that Customs Officers had been ordered to stop sending photographs (or samples) of suspect chips showing the information required by a manufacturer to authenticate a chip, even though CBP had been sending such photographs for nearly 8 years. Instead, CBP began sending redacted photos that obscured identifying information and left only the manufacturer's trademark visible. Given the advanced labeling technology now available to counterfeiters, manufacturers cannot determine whether chips are counterfeit based on these logo-only pictures. Unsurprisingly, before August 2008, seizures of counterfeit semiconductors were increasing year after year. Since CBP changed its policy, SIA members have reported receiving an increased number of complaints about counterfeits. Semiconductor manufacturers were not notified or provided an opportunity to comment before CBP began implementing the new policy: One day in August 2008, the identifying markings on photographs sent to manufacturers were simply redacted.

The CBP's new post-2008 redaction practice is based on an April 2000 Customs Directive [11] which instructed Customs Officers to "remove or obliterate any information indicating the name and/or address of the manufacturer, exporter, and/or importer, including all bar codes or other identifying marks" before providing samples of chips suspected to bear "confusingly similar" trademarks to semiconductor manufacturers. Of course, Customs Officers understood that this policy could not effectively prevent the importation of counterfeit semiconductors, and did not interpret the restrictive Directive to apply to photographs until August 2008 when, we have been told, CBP Port Officers were "reminded" by Treasury officials that the April 2000 Directive applies to photographs.

CUSTOMS NEEDS INDUSTRY SUPPORT TO PREVENT THE IMPORTATION OF COUNTERFEIT SEMICONDUCTORS

CBP cannot effectively prevent the importation of counterfeit semiconductors without the industry's assistance. A semiconductor is very different from apparel, for example, where a photograph of a fake Gucci handbag redacted per the Customs Directive's instructions likely still provides sufficient information for an intellectual property rights holder to determine the authenticity of merchandise. In contrast, semiconductor manufacturers use common exterior packages (which fit in common board sockets) for their semiconductors. Moreover, counterfeiters have obtained professional laser etching equipment to place fake codes on counterfeit chips. Thus, it is nearly impossible to determine whether a given chip is legitimate or counterfeit based on the redacted photographs.[12]

Semiconductor manufacturers can only assist CBP in preventing importation of counterfeit merchandise if CBP provides manufacturers with sufficient information to determine whether suspect chips are authentic. An unredacted photograph of a suspect chip would ordinarily be sufficient to provide the manufacturing codes (that usually represent lot numbers, dates, and locations of manufacture) that a manufacturer needs to authenticate a chip. Alternatively, CBP could provide manufacturers

[10] See note 8; Press Release, U.S. Department of Justice, Three California Family Members Indicted in Connection with Sales of Counterfeit High Tech Parts to the U.S. Military (Oct. 9, 2009), available at *http://www.justice.gov/criminal/cybercrime/aljaffIndict.pdf.*

[11] Customs Directive No. 2310–008A (April 7, 2000), available at *http://www.cbp.gov/linkhandler/cgov/trade/legal/directives/2310-008a.ctt/2310-008a.pdf.*

[12] See Exhibit 1.

with these numbers or a sample chip. However, a photograph that has been redacted to remove these numbers does not provide sufficient information to determine the authenticity of a chip. Unless CBP provides manufacturers unredacted photographs of suspect chips (or provides the manufacturing codes and dates and locations of manufacture reflected on the face of the suspect chips that only manufacturers can decipher), CBP cannot discharge its statutory obligation to ensure that imports comply with U.S. intellectual property laws. In such circumstances, the risk that counterfeit chips will enter U.S. commerce and ultimately end up as components in commercial, industrial, and military devices increases as we have witnessed since Treasury's policy shift.

CUSTOMS HAS THE AUTHORITY TO GET INDUSTRY HELP

The most frustrating aspect of the current policy is the fact that CBP has all the legal authority necessary to provide semiconductor manufacturers with the information necessary to stem the tide of counterfeit chips. Treasury officials have claimed that the 2000 Directive is meant to protect Customs Officers from liability under the Disclosure of Confidential Information ("DCI") provision of the Trade Secrets Act.[13] However, such protection is unnecessary, as Customs Officers are only exposed to DCI liability to the extent that CBP decides that information is confidential.[14] Therefore, CBP can effectively protect Customs Officers by simply declaring that the information included on the surface of semiconductors is not confidential information, as it had implied prior to its policy shift. Indeed, it is unclear how a code that is readily visible to anyone looking at the product label on a container containing semiconductors or the surface of a semiconductor can be confidential information. Tellingly, when Customs promulgated the rule that the 2000 Directive was intended to "fix,"[15] it identified two potential trade secrets that might be divulged when disclosing information: The identity of the manufacturer and the identity of the importer.[16] But sharing the codes on the surface of semiconductors and product labels on the packaging with semiconductor manufacturers would not reveal either, as the manufacturer knows its own identity and the surface codes reveal no information about a chip's importer.

CBP has failed to understand that even if the publicly viewable codes were confidential, Congress clearly contemplated CBP disclosing such information to rights holders in order to permit CBP to fulfill the many laws and treaties requiring it to stop counterfeits from entering the United States. The DCI simply prohibits Government officials from disclosing confidential information that "concerns or relates to . . . the identity . . . of any person" to "any extent not authorized by law." Accordingly, Congress has authorized CBP to provide unredacted photos to semiconductor manufacturers through the Tariff Act of 1930, the Lanham Act, the North American Free Trade Agreement and the GATT Agreement on Trade-Related Aspects of Intellectual Property Rights. In addition, CBP's own Disclosure of Information Regulation authorizes such disclosure.[17] It is truly difficult to understand why CBP believes disclosing information to semiconductor manufacturers is unlawful when ICE, DOD, DOJ, NCIS, and even the FBI—the agency tasked with enforcing the Trade Secrets Act—do not, and in fact routinely disclose such information to semiconductor manufacturers.

CONCLUSION

As a trade association that represents one of America's most vital industries, SIA hopes that all executive agencies will support the Obama administration's intellectual property enforcement efforts by resolving this counterfeit issue expeditiously.

---

[13] 18 U.S.C. § 1905.

[14] In *United States* v. *Wallington,* 889 F.2d 573 (5th Cir. 1989), the Fifth Circuit logically found that the DCI only prohibits the disclosure of confidential information. In addition, the Fifth Circuit clarified that Customs agents cannot be held liable for DCI violations without "at least . . . knowledge that the information is confidential in the sense that its disclosure is forbidden by agency official policy (or by regulation or law)." Thus, since the Trade Secret Act does not address the information at issue, CBP Officers could be shielded from any potential DCI liability (to the extent such liability may exist) with a stroke of a pen if CBP were to clarify the Directive to permit Customs agents to share with semiconductor manufacturers unredacted photographs.

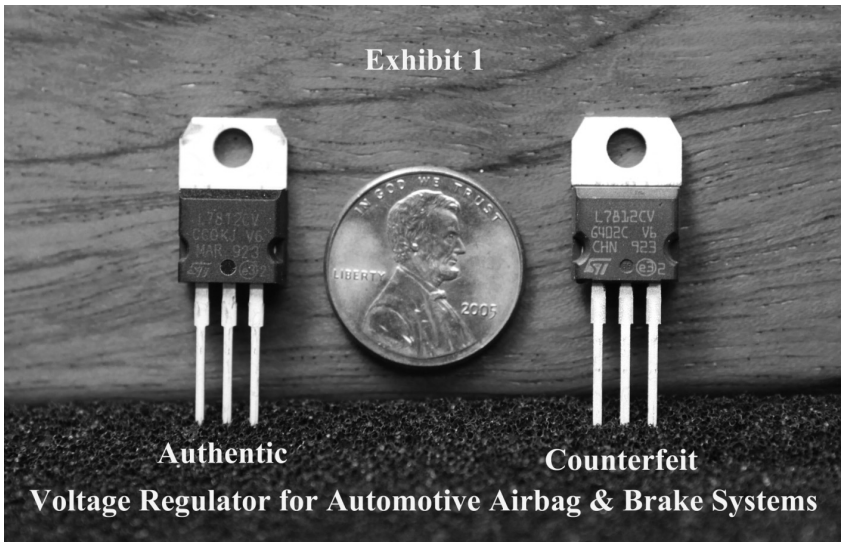
[15] 19 C.F.R. § 133.25 ("Customs may disclose to the owner of the trademark or trade name . . . in order to obtain assistance in determining whether an imported article bears an infringing trademark or trade name . . . [a] description of the merchandise").

[16] Copyright/Trademark/Trade Name Protection; Disclosure of Information, 63 Fed. Reg. 11996, 11997 (Mar. 12, 1998); see also Gray Market Imports and Other Trademarked Goods, 64 Fed. Reg. 9058 (Feb. 24, 1999).

[17] See note 15.

Counterfeit semiconductors are a clear and present National security threat and danger to human health because they are used in many mission-critical applications. SIA is pleased with the efforts by the U.S. Attorney for the District of Columbia, ICE, NCIS, and other Federal law enforcement agencies to bring to justice unscrupulous brokers selling dangerous counterfeits into the civilian and military supply chain. However, the 2000 CBP policy, further refined in 2008, prevents the U.S. Government from most effectively working with industry to prevent counterfeit chips from being imported into the United States. This is alarming, especially given the danger such chips so obviously present.

We respectfully request this subcommittee and Congress to work with CBP and Treasury to ensure that the pre-2008 practice of sharing unredacted pictures of suspected counterfeit semiconductors and product labels with manufacturers is reinstated in the interest of safeguarding the health and safety of the American public and our military.



Mr. MCCAUL. Thank you.

Mr. Toohey, I will ask in my questions why DHS changed that practice. I don't know how you can identify with the markings taken off. So it seems a bit absurd to me, but we will follow up with that in questions.

Mr. Russo, you are now recognized.

STATEMENT OF MICHAEL RUSSO, DIRECTOR, GLOBAL SECURITY AND PRODUCT PROTECTION, ELI LILLY AND COMPANY

Mr. RUSSO. Good morning, Mr. Chairman and Members of the committee.

First, let me thank the committee for inviting Eli Lilly to testify about the dangers of counterfeit pharmaceuticals and the efforts of ICE and CBP to stop these products which have serious consequences for Americans, global public health, our economy, National security, and certainly our industry. In order to meet time constraints, I will request that my full testimony be submitted for the record, and I will provide a summary of my comments today.

I am Michael Russo, director of global security and asset protection for Eli Lilly and Company, a global pharmaceutical company. Lilly invests heavily to research, develop, and manufacture safe and effective pharmaceutical therapies which treat many diseases

and save lives. Criminal counterfeiters steal those innovations by copying our branding attributes, packaging characteristics, and deliberately misleading consumers to believe they are buying our legitimate, safe, quality-controlled medicines. Our analysis of counterfeits have determined that in many cases they are poorly made, lack efficacy, and may contain dangerous and other unknown substances. There are several known cases in which counterfeit products have been responsible for patient deaths.

We are also seeing that the problem is on the rise globally. We have learned from our work that many counterfeiters are highly sophisticated and are associated with international organized crime networks. For this reason, the United States and other governments must continue to work and dismantle these organizations before the counterfeit drug trade extends so broadly that it undermines the legitimate global pharmaceutical supply. Lilly is committed to assisting Government agencies like ICE in tackling this threat.

In short, ICE and CBP have been highly supportive and responsive to our concerns, though we all need to increase efforts and do more. Their efforts have resulted in numerous criminal convictions and a significant number of seizures of counterfeit pharmaceuticals at our borders. Through their efforts we have seen an increased cooperation of foreign law enforcement agencies that target counterfeit operations outside the United States.

The effectiveness of ICE has been the result not only of work of numerous individual ICE agents globally, but also the critical coordination and support provided by the IPR Center. The internet has posed a significant challenge by facilitating criminal counterfeiting. ICE has responded to complaints by brand owners with Operation in Our Sites II, a new approach to the internet trade in counterfeits. These actions sent a message that the internet was no longer a safe haven for the distribution of counterfeit product. We would like to see more attention by this committee and other relevant U.S. Government agencies to the dangerous counterfeit pharmaceuticals that are being sold on the internet.

Customs and Border Protection officers have also increased their efforts to combat counterfeit pharmaceuticals. There are thousands of illegal small parcels and express mail packages entering the United States every day facilitated by illegitimate on-line drug sellers posing as legitimate pharmacies. We support continuing and increasing high-profile interdiction operations, as well as using the collection of data to inform and educate Americans about the dangers of purchasing medicines on-line.

International cooperation aimed at coordinated law enforcement operation and training is another vital element of how ICE is contributing to this problem. We support continued and expanded posting of ICE and CBP attachés outside the United States, and encourage effective resourcing to enable an increase in focus on counterfeit pharmaceuticals given their unique threat.

The efforts by ICE to combat counterfeit pharmaceuticals are noteworthy, but going forward, more needs to be done to protect Americans. We view the following as key areas of concern and additional focus going forward.

More operations and public education is needed to disrupt thousands of illegal shipments entering the United States daily. CBP needs more resources and technology to interdict these shipments, and all appropriate agencies need authority to destroy the known counterfeits and illegal drugs instead of shipping them back to the criminals who are sending them to our country.

More attention needs to be focused on a broad internet strategy to address thousands of illegal websites that are selling fake and dangerous pharmaceutical products to U.S. patients.

We believe a major public awareness campaign is needed to educate citizens about the dangers of fake products and the importance of purchasing medicines safely on the internet. The FDA and IPEC are working to develop a coordinated education effort.

DHS has the unique ability to contribute to this campaign by providing real data about what is coming across our borders.

Additionally, more should be done to encourage the voluntary efforts initiated by Google and Go Daddy in their Center for Safe Internet Pharmacies to stop providing services to illegal on-line drug sellers and distributors of counterfeit drugs. Their efforts have the potential to drastically reduce the threat posed to patients and reduce the burden on law enforcement agencies. Therefore, we encourage this committee to support more voluntary efforts.

As a final part of internet strategy, more effort is needed through investigation to track websites back to the source of supply and to major distributors of counterfeit medicines. This requires increased international law enforcement cooperation in response to leads developed and aggressive law enforcement action when justified.

In this spirit we support and encourage the on-going work of the IPR Center to bring together the various Government authorities and brand holders to fight this criminal activity that is endangering our homeland and National security. It is critical that all of the relevant agencies, ICE, CBP, the FDA, the FBI, and local authorities, are working together with the utmost coordination to fight the counterfeit drug trade. Counterfeit pharmaceuticals pose a very unique and frightening threat and must not be viewed as an economic or IP crime alone.

In conclusion, I want to underscore that combating counterfeited pharmaceuticals is a very complex issue requiring the cooperation of many agencies and governments, as well as the private sector, health care professionals, and nongovernment organizations. None of us can do this alone.

I might also add, Mr. Chairman, that DHS and ICE get this situation. Just 2 weeks ago we were summoned to New York to meet with Secretary Napolitano, who was focusing on this matter, and additional resources from her team are being added to this as we see it.

We stand with you in the effort to protect U.S. consumers and the homeland from counterfeit medicines. There is a lot of work needed, and we believe that it is vital to the mission of preventing crime and protecting patients.

Again, I thank the committee for inviting Lilly to testify today and look forward to any of your questions.

Mr. MCCAUL. Thank you, Mr. Russo.

[The statement of Mr. Russo follows:]

PREPARED STATEMENT OF MICHAEL RUSSO

JULY 7, 2011

Good morning, Mr. Chairman and Members of the subcommittee. First, let me thank the committee for inviting Lilly to testify about the dangers of counterfeit pharmaceuticals and the efforts of ICE and CBP to stop these dangerous products which have serious consequences for Americans, global public health, our economy, National security, and certainly our industry. In order to meet time constraints, I will request that my full testimony be submitted for the record, so that I can provide a summary of my comments today.

I am Michael Russo, Director of Global Security Product and Asset Protection for Eli Lilly and Company, a global researched-based pharmaceutical company based in Indianapolis. Lilly invests heavily to research, develop, and manufacture safe and effective pharmaceutical therapies which treat many diseases and save lives. Criminal counterfeiters steal those innovations, by copying our branding attributes and packaging characteristics and deliberately misleading consumers to believe they are buying and using the legitimate, safe, quality-controlled products that we manufacture. In our experience with counterfeit products, we have observed that in many cases they are poorly made in filthy facilities, lack efficacy, and may contain dangerous and other unknown substances. There are several known cases in which counterfeit products have been responsible for patient deaths. And it is likely that counterfeit medicines have inadvertently caused a patient harm by denying the effective treatment of a genuine medicine.

We are also seeing that the problem is on the rise globally. Criminals cannot resist the allure of extremely high profits and surprisingly low risks associated with counterfeit pharmaceuticals. They are producing counterfeit versions of expensive and innovative anti-cancer drugs, as well as less expensive generic medicines such as antibiotics and vaccines. They target developed markets in the United States and Europe, but also sell fake medicines to some of the poorest populations, in some cases contributing to drug-resistant strains of disease. I mention this because it is important to understand that this is a crime against global public health, not just our company, and not just our country. It threatens all of us, whether you buy medicine from a fake on-line pharmacy, or you are administered a counterfeit vaccine. If the fake products continue to proliferate; theoretically, they could overtake genuine product in some countries, and that is frightening.

For these obvious implications on public health, our company has prioritized the issue, acting as an industry leader to raise the matter with U.S. agencies and other governments. We have established a coordinated team of Lilly professionals who analyze the problem and directly assist U.S. and foreign governments in the fight against counterfeit pharmaceuticals. We also chair our industry association's Anti-Counterfeiting Working Group, working through PhRMA and in partnership with other sectors to combat this threat.

We have learned from our work that the counterfeiters are highly sophisticated and are associated with international organized crime networks. While our companies work to comply with numerous laws and regulations to ensure our medicines are safe for patients, criminal networks circumvent all of them with no concern for the patient's health or our company's brand. They are pretending to be us, but they do not regulate or control the quality of their products, and our patients suffer the consequences.

For this reason, the United States and other governments must continue work to disrupt and dismantle these organizations before the counterfeit drug trade extends so broadly that it undermines the legitimate global pharmaceutical supply.

Lilly is committed to assisting Government agencies like ICE in tackling this threat. Lilly investigators work globally to develop information regarding the various manufacturing and distribution networks involved in the counterfeit pharmaceutical trade and the individuals responsible for them. In order to succeed, we turn this information over to a law enforcement agency capable of developing the information we provide and ultimately bringing those responsible to justice. ICE and CBP have been highly supportive and responsive to our referrals. Their efforts have resulted in numerous criminal convictions and a significant number of seizures of counterfeit pharmaceuticals at our borders. Through their efforts, we have seen an increase in cooperation with foreign law enforcement agencies that target counterfeit operations outside the United States.

The effectiveness of ICE has been the result of not only the work of numerous individual Homeland Security Investigative (HSI) agents globally, but also the critical coordination and support provided by the National Intellectual Property Rights Coordination Center (IPR Center) which has served as a model of interagency and

public-private coordination for Government agencies and brand holders here in the United States. The IPR Center maintains continuous communication with brand owners and uses the expertise of its member agencies to share information, test new initiatives, coordinate enforcement actions, and conduct joint investigations. It also provides an effective forum for brand owners to share information directly with investigative professionals familiar with counterfeit/intellectual property (IP) crime and for us to provide training regarding the characteristics of our products.

The efforts by ICE to combat counterfeit pharmaceuticals have resulted in several criminal convictions. In 2009, Kevin Xu was convicted and sentenced in U.S. District Court in Houston for distributing counterfeit and misbranded pharmaceuticals. Xu's criminal activities resulted in him profiting in the amount of $1.5 million in 1 year from the sale of counterfeit pharmaceuticals. He was also responsible for distributing counterfeits in Europe which resulted in the recall of three pharmaceutical products. In Houston, Lawrence Chow was sentenced to 12 months and one day for conspiring to distribute counterfeit pharmaceuticals and trafficking in pharmaceuticals bearing false labeling and counterfeit trademarks. In St. Louis this February, Mark Hughes was sentenced to 48 months in Federal prison on multiple charges including the sale of counterfeit and misbranded pharmaceuticals. These convictions send an important deterrent message to criminals who engage in this activity. We are thankful for and support additional criminal investigations and resulting prosecutions to send a clear message to drug counterfeiters who target the United States and elsewhere. That said, the convictions are paltry compared to the severity of the offense and do not send a strong enough message to future criminals.

As this committee may know, the internet has posed a significant challenge by facilitating criminal counterfeiting. It is used as a conveniently anonymous platform by manufacturers, distributors, and buyers of counterfeit pharmaceuticals. Criminal organizations dupe customers into buying counterfeits through fake on-line "pharmacies" which use trademarked images of branded pharmaceutical products. In response to this, ICE has responded to complaints by brand owners with Operation in Our Sites II—a new approach to the internet trade in counterfeits. In late 2010, the Justice Department Criminal Division, ICE and nine U.S. Attorneys' offices across the country executed seizure orders against 82 internet domain names of websites engaged in the sale and distribution of counterfeit goods and illegal copyrighted works. These actions sent a message that the internet was no longer a safe haven for the distribution of counterfeit product. We would like to see more attention by this committee and relevant U.S. Government agencies to the number of dangerous counterfeit pharmaceuticals that are being sold on the internet. Law enforcement operations such as Operation in Our Sites are crucial deterrents, but more must be done to take down fake on-line pharmacy sites and interdict incoming shipments from these sites. This will undoubtedly require more active support from the private sector companies that are indirectly facilitating the registration and advertisement of new sites every day as well as processing and shipping the purchased fake and illegal medicines through their services. They can do a lot to support law enforcement and prevent this criminal activity. We endorse the excellent work of the Intellectual Property Enforcement Coordinator (IPEC), Victoria Espinel, in fostering this collaboration and seeking ways to work more robustly with the private sector as part of her Joint Strategy. We also endorse the work of the Alliance for Safe Online Pharmacies (ASOP) *(www.safeonlinerx.com)* of which Lilly is a member.

International cooperation aimed at coordinated law enforcement operation and training is another vital element of how ICE is working to address this problem. In addition to operations and trainings conducted through such multi-lateral institutions as the Asia Pacific Economic Cooperation (APEC), there is regular bilateral engagement through the ICE and CBP Attaché's posted in U.S. Embassies. These attachés are critical to the success of international counterfeit pharmaceutical investigations. They develop the critical links and relationships with foreign law enforcement authorities that are necessary to effectively dismantle counterfeit networks. In addition, they provide brand owners with a professional investigative resource in-country with whom to discuss and refer cases. ICE attachés coordinate important training between local authorities and brand owners that increase the importance and awareness of IP crimes and familiarize local authorities with the dangers of counterfeit pharmaceuticals and how these products can harm local populations. We support the continued and expanded posting of ICE and CBP attaches outside the United States and we encourage effective resourcing to enable an increase in focus on counterfeit pharmaceuticals, given the unique threat they pose to global public health and our own National security.

Customs and Border Protection (CBP) officers who inspect the millions of shipments entering the United States have also increased their efforts to combat counterfeit pharmaceuticals. There are thousands of illegal small parcels and express

mail packages entering the United States every day facilitated by illegitimate on-line drug sellers posing as legitimate pharmacies. CBP officers have effectively responded to our concerns about these shipments by implementing coordinated efforts to inspect large volumes of packages for counterfeits and referring those in violation to ICE HIS agents for follow-up. Lilly, along with other industry partners, provided product identification training as well as on-site analysis of seized products. These efforts are critical to protecting U.S. consumers. They send an important deterrent and educational message to U.S. consumers. We support continuing and increasing high-profile interdiction operations, as well as using the collection of data to inform and educate Americans about the dangers of purchasing medicines on-line.

The efforts by ICE to combat counterfeit pharmaceuticals are noteworthy but going forward more needs to be done to protect Americans. We view the following as key areas for concern and where we recommend additional focus going forward:

- More operations and public education is needed to disrupt the thousands of illegal shipments entering the United States daily in small parcels and express mail. CBP needs more resources and technology to interdict these shipments and all appropriate agencies need the authority to destroy the known counterfeit and illegal drugs seized instead of shipping them back to the criminals who are sending them to our country. We refer to the March 2011 administration's White Paper on Intellectual Property Enforcement Legislative Recommendations and Counterfeit Pharmaceutical Interagency Working Group Report to the Vice President and Congress, which provided important insight and suggestions related to this challenge.
- We recommend legislation to increase penalties for counterfeit and diverted products, which pose a direct threat to public health and safety. Increased penalties will help to send an important message to criminals engaged in counterfeiting pharmaceuticals.
- More attention needs to be focused on a broad international internet strategy to address the thousands of illegal websites that are selling fake and dangerous pharmaceutical products to U.S. patients. We are currently providing ICE with lists of offending internet websites which are infringing on our trademarks and placing patients at risk. While their investigative/deterrent work continues, more must be done with education and voluntary action to compliment that effort.
- As part of this strategy, we believe a major public awareness campaign is needed to educate citizens about the dangers of fake products and the importance of purchasing medicine safely on the internet. The FDA and IPEC are working to develop a coordinated education effort, and we believe that funding and resources for this kind of a campaign are critical to preventing this crime and protecting the homeland. Though Government funding is needed to kick-start the effort, its success requires the participation of several stakeholders, from non-governmental organizations such as patient advocates, to health-care professionals such as doctors, nurses, and the local pharmacist. It must be a comprehensive education effort to inform people about the dangers of fake drugs and why they should go through legitimate channels when purchasing medicines.
- DHS has the unique ability to contribute to this campaign by providing real data about what is coming across our borders as well as information about the true nature of the criminal organizations involved in the fake drug trade. DHS is needed to help tell the story of the criminals involved in making fake medicines in order to educate the public and health care professionals.
- Additionally, more should be done to encourage and realize outcomes from the voluntary initiative of companies like Google and Go Daddy to stop providing services to illegal on-line drug sellers and distributors of counterfeit drugs. Google and Go Daddy have initiated a new nonprofit called the Center for Safe Internet Pharmacies (CSIP) with membership that includes search engines, domain name registrars, credit card companies, and shippers. CSIP is a vital development in efforts to reduce this crime on the internet over the long term, and it is an important compliment to the day-to-day work that ICE is doing. CSIP has the potential to drastically reduce the threats posed to patients and reduce the burden on law enforcement agencies; therefore, we encourage this committee to support the work that CSIP is doing.
- Specifically, we ask for your support of the section in the Protect IP Act of 2011 (S. 968) which provides legal immunity to CSIP and other internet-related companies who stop providing services to websites that endanger the public health. No House version has been introduced yet, but that section would be very helpful in any final House legislation. It helps to remove any final disincentive to voluntary action that will protect American citizens.

- As a final part of the internet strategy, more effort is needed through investigations to track websites back to the source of supply and the major distributors of counterfeit medicines. This requires increased international law enforcement cooperation in response to leads developed and aggressive enforcement action to follow up when justified. The counterfeit drug trade is providing enormous profit that fuels other dangerous criminal activity by organized criminal networks. Dismantling these counterfeit pharmaceutical networks must become a higher priority for law enforcement agencies globally.
- In this spirit, we support and encourage the on-going work of the IPR Center to bring together the various Government authorities and brand holders to fight this criminal activity that is endangering our homeland and National security. It is critical that all of the relevant agencies, ICE and CBP, the FDA, the FBI, and local authorities, are working together with the utmost coordination to fight the counterfeit drug trade. This growing threat of counterfeit pharmaceuticals poses a very unique and frightening threat, and it must not be viewed as an economic or IP crime alone.

In conclusion, I want to underscore that combating counterfeit pharmaceuticals is a very complex issue requiring the cooperation of many agencies and governments, as well as the private sector, health care professionals, and non-government organizations. None of us can do it alone. We stand with you in the effort to protect U.S. consumers and the homeland from counterfeit medicines and dismantle the international crime networks that profit from the counterfeit drug trade. There is a lot of work needed, and we do believe it is vital to the mission of preventing crime and protecting patients everywhere. Again, I thank the committee for inviting Lilly to testify today and for your commitment to this important issue and look forward to any questions.

Mr. MCCAUL. The Chairman now recognizes Mr. Mancuso for 5 minutes.

STATEMENT OF MARIO MANCUSO, PARTNER, FRIED, FRANK, HARRIS, SHRIVER & JACOBSON LLP

Mr. MANCUSO. Thank you, Chairman McCaul, Ranking Member Thompson, and distinguished Members of the subcommittee. Thank you for the opportunity to testify today.

Today's hearing is a timely and important one and implicates a number of vital U.S. National interests, our technological competitiveness, U.S. jobs, and our Nation's security.

As an initial matter, I believe we are fortunate to have talented and committed career civil servants in our Government, including at DHS. Unfortunately, this alone is not enough to either keep U.S. industry globally competitive or dangerous technologies out of the hands of U.S. adversaries. Ironically, we need to do both more and less, and we might start by raising our expectations for what constitutes success in the export control context.

In my view, we should seek to enhance U.S. National security and remain the most competitive, the most innovative economy in the world. That objective is not merely desirable; it is vital, and it is possible.

Before giving my general observation about DHS' role in export control enforcement, I would like to simply describe the context in which export control policy and enforcement take place.

The world has changed since the end of the Cold War, and it is changing still. Globalization is reordering our world, and certain facets of globalization, economic, technological, and political, are impacting our Nation's security profile and shaping the exercise of our National power.

Today's National security threats are more numerous and varied than ever before, and they require more and more differentiated approaches to mitigate risk to U.S. security interests. At the same

time, the global, economic, and competitive landscape has changed profoundly, fundamentally realtering the efficacy and opportunity costs of export controls.

Indeed, the very success of our economic diplomacy, the end of the Cold War, and globalization generally, has increased the pool of world-class competitors and altered the dynamics of global economic competition. Unlike when U.S. export controls were originally instituted, technology, talent, and capital are now ubiquitous. Today U.S. companies compete with the rest of the world, including companies in China and in India, but also in Brazil, Korea, Indonesia. The list goes on.

Consider two startling facts. In 2009, King Abdullah University opened its doors in Saudi Arabia. On the day it opened, it had an endowment roughly equivalent to that of MIT, except it took MIT 142 years to get there. Today it is estimated that 90 percent of all scientists and engineers live in Asia.

But there is more. The alchemy of our military technological superiority has also changed. In the past, approximately two-thirds of our Nation's military technologies were developed in defense-unique R&D settings with the remaining third generated from adaptations of commercial, off-the-shelf technologies. Today those proportions are almost exactly reversed. Thus, in a very real way, the vitality of our civilian technology industry is now linked to U.S. National security.

In the aggregate these developments are not altogether a bad thing. In fact, the United States welcomes the integration of developing countries into a rules-based global economy, but these changes have challenged the core assumption of export controls, that we have something that other people do not have, that complicated the calculus of export controls generally and further elevated the salience of U.S. economic competitiveness and technology leadership in National security policymaking.

To some degree, U.S. export control regulations impact the competitiveness of U.S. industry and, therefore, jobs in America. To the extent that such export controls actually advance U.S. security interests, those export controls are necessary. However, to the extent that such controls create protected foreign markets for U.S. competitors without advancing U.S. security interests, they should be reconsidered, unless doing so would be inconsistent with other important U.S. National interests.

While this broader policy calculus is really beyond the scope of this hearing, it should nonetheless inform DHS' enforcement work. On a surface level, DHS has impressive institutional tools at its disposal: A large pool of special agents, fulsome legal authorities to conduct export control investigations here and abroad, and a network of law enforcement personnel deployed around the world. Yet, thus far, DHS' enforcement results appear to be modest in comparison to its resources. In this connection I offer the following practical observations.

First, it is not only about DHS. DHS is an important actor in export control enforcement, but it is not the only one. While there is generally effective coordination at the senior policy and special agent level, there could be improved coordination at the middle-management level of the various departments and agencies with

export control responsibilities. Indeed, our Nation's success in export control enforcement matters at all is largely attributable to the make-it-happen attitude of special agents in the field, and while President Obama's creation of an export control coordination center is a good idea, it will not, by itself, guarantee a positive result.

Second, DHS should improve its export control enforcement acuity and operational concept. Large parts of DHS' investigative culture developed around the investigation of very different kinds of cases. As a result, export control acumen is not a prominent part of the DHS investigative self-identity. This is not an insuperable obstacle, but it will require organizational leadership to ensure that export control expertise remains a visible and highly regarded DHS capability.

Third, DHS should strengthen its enforcement architecture.

Fourth, DHS should refocus its enforcement activities. No entity, including the Department of Homeland Security, can do everything everywhere all the time. This is particularly true in a resource-constrained environment. DHS should refine its classified intelligence gathering and analysis capability and prioritize its efforts accordingly. This should be done periodically to ensure that DHS is focusing in the geographic and other areas of maximum National consequence.

Finally, DHS should accelerate its engagement with allied and partner governments to help address our shared security interests. DHS should accelerate and elevates its engagement with other governments through its attaché presence around the world. While it should seek to work with all governments of goodwill, it should prioritize its efforts based on their contribution to U.S. and international security. This important work should be closely coordinated with the U.S. State Department and, in every case, with our Chiefs of Mission abroad.

Thank you for your kind attention. I understand I went over my limit, but I would be pleased to answer any questions you may have. Thank you.

[The statement of Mr. Mancuso follows:]

PREPARED STATEMENT OF MARIO MANCUSO

JULY 7, 2011

Chairman McCaul, Ranking Member Thompson, and distinguished Members of the subcommittee: Thank you for the opportunity to testify today. Today's hearing, "Homeland Security Investigations: Examining DHS's Efforts to Protect American Jobs and Secure the Homeland," is a timely and important one, and implicates a number of vital U.S. National interests—our technological competitiveness, jobs, and our Nation's security.

I have been fortunate to have had the opportunity to consider these issues from a variety of perspectives in the public and private sector—as Deputy Assistant Secretary of Defense for Special Operations, as Under Secretary of Commerce for Industry and Security in the administration of President George W. Bush, and as an international lawyer counseling clients in export control and related matters. I hope my testimony today will be of some value to the Members of this subcommittee as you continue your important work in assessing the efficacy and multiple impacts of DHS investigations.

As an initial matter, I believe we are fortunate to have talented and committed career civil servants in our Government, including at DHS. Unfortunately, this alone is not enough to either keep U.S. industry globally competitive or dangerous technologies out of the hands of U.S. adversaries.

Ironically, we need to do both more and less. And, we might start by raising our expectations for what constitutes "success" in the export control context. In my view, we should seek to enhance U.S. National security and remain the most competitive, the most innovative economy in the world. That objective is not merely desirable, it is absolutely vital—and possible to achieve.

Before giving my general observations about DHS's role in export control enforcement, I would like to simply describe the context in which export control policy and enforcement take place.

THE POLICY CONTEXT

The world has changed since the end of the Cold War, and it is changing still. Globalization is reordering our world and certain facets of globalization—economic, technological, and political—are impacting our Nation's security profile, and shaping the exercise of our National power.

Today's National security threats are more numerous and varied than ever before, requiring more and more differentiated approaches to mitigate risk to U.S. security interests. At the same time, the global economic and competitive landscape has changed profoundly, fundamentally re-altering the efficacy and opportunity costs of export controls.

Indeed, the very success of our post-war economic diplomacy, the end of the Cold War, and globalization generally, has increased the pool of world-class competitors and altered the dynamics of global economic competition. Unlike when U.S. export controls were instituted, technology, talent, and capital are now ubiquitous. Today, U.S. companies compete with the rest of the world, including companies in China and India, but also in Brazil, Korea, Indonesia—and the list goes on.

Consider two startling facts:

- In 2009, King Abdullah University opened its doors in Saudi Arabia. On the day it opened it had an endowment roughly equivalent to that of MIT—except it took MIT 142 years to get there.
- Today, it is estimated that more than 90% of all scientists and engineers live in Asia.

But there's more. The very alchemy of our military technological superiority has also changed. In the past, approximately two-thirds of our Nation's military technologies were developed in defense-unique R&D settings, with the remaining one-third generated from adaptations of commercial, off-the-shelf technologies. Today, those proportions have been almost exactly reversed. Thus, in a very real way, the vitality of our civilian technology industry is now linked to U.S. National security.

In the aggregate, these developments are not altogether a bad thing. In fact, the United States welcomes the integration of developing countries into a rules-based global economy. But these changes have: (i) Challenged the core assumption of our export controls—i.e., that we have something that others do not, (ii) complicated the net-benefit calculus of export controls generally, and (iii) further elevated the salience of U.S. economic competitiveness and technology leadership in National security policymaking.

In this environment, we can no longer assume that export controls always and automatically work to enhance U.S. security interests. Instead, we must be discerning in the application of export controls, rigorous in our enforcement of a right-sized export-control regime, and mindful of the long-term relationship between U.S. security interests and U.S. technology competitiveness.

To some degree, U.S. export control regulations impact the competitiveness of U.S. industry—and therefore, jobs—in America. To the extent that such export controls actually advance U.S. security interests, those export controls are necessary. However, to the extent that such controls create protected foreign markets for U.S. competitors without advancing U.S. security interests, they should be reconsidered.[1]

While this broader policy calculus is beyond the scope of this hearing (and the mandate of DHS enforcement officials), it should nonetheless inform the tenor of DHS's enforcement work.

DHS AND EXPORT CONTROL ENFORCEMENT

On a surface level, DHS has impressive institutional tools at its disposal: A large pool of highly-trained special agents, fulsome legal authorities to conduct export control investigations here and abroad, and a network of law enforcement personnel deployed around the world. Yet, thus far, DHS's enforcement results appear to be modest by comparison to its resources.

In this connection, I offer the following observations:

---

[1] Unless doing so would be inconsistent with other U.S. National interests.

First, it's not only about DHS.

DHS is an important actor in export control enforcement, but it is not the only one. While there is generally effective coordination at the senior policy and special agent level, there could be improved coordination among the middle-management levels of the various departments and agencies with export control responsibilities. Indeed, our Nation's success in export control enforcement matters is largely attributable to the "make it happen" attitude of our special agents in the field. And, while President Obama's creation of an Export Control Coordination Center (ECCC) is helpful, it will not guarantee a positive result in this regard.

Second, DHS should improve its export control enforcement acuity and "operational concept."

Large parts of DHS's investigative culture developed around the investigation of very different kinds of cases (e.g., border security, human trafficking, bulk cash smuggling). As a result, export control acumen is not a prominent part of the DHS investigative self-identity. This is not an insuperable obstacle, but it will require organizational leadership to ensure that export control expertise remains a visible, and highly-regarded, DHS capability.

In addition, DHS has historically focused its export control enforcement efforts on detecting illegal exports, investigating potential violations, and obtaining international cooperation to investigate leads abroad. This approach is reasonable but may lead to sub-optimal enforcement results by not fully leveraging the informational resources of the private sector. DHS should, therefore, refine and build upon Project Shield America to better inform private industry of export control issues and to more effectively engage the private sector as a full partner.

Third, DHS should strengthen its enforcement architecture.

Though it did not resolve thorny jurisdictional and other issues, President Obama's creation of the ECCC is a promising initiative to enhance interagency coordination and limit duplicative or conflicting enforcement activities. But, even a Presidential Executive Order is of limited utility without consistent day-to-day leadership attention and without appropriate DHS prioritization. Indeed, in the absence of leadership involvement, the ECCC could make matters worse if it only adds organizational complexity without operational value.

Fourth, DHS should refocus its enforcement activities.

No entity, including DHS, can do everything, everywhere, all the time. This is particularly true in a resource-constrained environment. DHS should refine its classified intelligence gathering and analysis capability, and prioritize its enforcement efforts accordingly. This should be done periodically, to ensure that DHS is focusing in the geographic and other areas of maximum National consequence.

Finally, DHS should accelerate its engagement with allied and partner governments to help address our shared security interests.

DHS should accelerate and elevate its engagement with other governments through its attaché presence around the world. While it should seek to work with all governments of good will, it should prioritize and rationalize its efforts based on their contribution to U.S. and international security interests (e.g., WMD proliferation). This important work should be closely coordinated with the U.S. State Department and, in every case, with our Chiefs of Mission abroad.

Thank you for your kind attention. I would be pleased to answer any questions that you may have at this time.

Mr. MCCAUL. Thank you, Mr. Mancuso.

The Chairman now recognizes Ms. McNeill for 5 minutes.

STATEMENT OF JENA BAKER MC NEILL, PRIVATE CITIZEN

Ms. BAKER MCNEILL. Chairman McCaul, Ranking Member Thompson, and subcommittee Members, thank you for this opportunity to testify today. I should state beforehand, as Chairman McCaul expressed, that these views are my own and not an official position of The Heritage Foundation.

I hope to make three points today. First, worksite enforcement is vital to our Nation's security, economic well-being, and rule of law. The Obama administration, however, has used its tenure to roll back or deemphasize several key worksite enforcement measures.

Second, the Department of Homeland Security's employer-focused strategy for worksite enforcement is inadequate in terms of creating a legal workforce in the United States, and it really sends the message that the Government does not take enforcement of our immigration laws seriously.

Third, the right worksite enforcement strategy will address both employers of illegal labor and illegal workers alike, deploying a menu of enforcement tools aimed at stopping all forms of illegal employment, which largely include identity theft, fake documentation, and off-the-books employment.

While the employment of illegal workers has been unlawful in the United States since 1986, these laws were not seriously enforced. From 2004 to 2008, the Bush administration set up a strategy to ramp up worksite enforcement of immigration laws, including initiatives aimed at both employers of illegal labor and illegal workers.

One of the more well-known of these actions was commonly referred as to worksite raids. Law enforcement and immigration authorities, pursuant to a criminal investigation, would arrive unannounced at workplaces suspected of employing illegal immigrants. Illegal immigrants would then be turned over to law enforcement, while employers would then be prosecuted. These checks were a huge deterrent mechanism to those seeking to avoid the law.

Other efforts used by the administration at the time included expanded use and promotion of E-Verify, as well as an effort to use Social Security no-match letters as an enforcement tools. These efforts, I think, were good first steps towards effectively identifying individuals working illegally and employers that were abusing immigration laws.

The Obama administration has since announced a change in strategy, taking emphasis off of identifying illegal workers and on punishing employers of illegal labor. The administration has, for instance, avoided worksite raids and has focused its efforts on I–9 audits where employers have lead time by which to clear out a staff of illegal labor. Even upon auditing, employers are largely oftentimes free of further investigation as long as they are doing the rote technicality of filling out the I–9 forms appropriately, even if they are aware that rampant identity theft could be going on in their workplace.

Essentially, with plenty of notice, it is fairly easy for most employers to clean up their payroll to pass the Obama's administration's muster. With less threat of criminal punishment, they can pass off any civil fines they receive as just another cost of doing business. While these audits look great on paper, they do very little in terms of actually enforcing immigration laws.

These actions are also missing out on an opportunity to identify and hold accountable illegal workers. Instead, now they can go down the street and find another job illegally. This pattern sends a message that we don't take enforcement seriously, but it also hinders enforcement efforts because apprehended illegal workers were often helpful to investigators in a prosecution of employers who were abusing the law.

The administration has also expressly abandoned the effort to use no-match as an enforcement tool and has been active in trying

to roll back implementation of REAL ID. Given that identity theft is one of the biggest challenges facing worksite enforcement, setting minimum standards for driver's licenses just makes sense. However, the administration has spent more time trying to get the act repealed or replaced than on meeting its own implementation deadlines.

Meanwhile, the administration has made E-Verify the centerpiece of its worksite enforcement efforts. Let me emphasize: E-Verify is an outstanding tool for catching the use of fake identification by illegal workers, but it is not a silver bullet solution for enforcement. For instance, it can't catch off-the-books employment or situations of identity theft.

If DHS is serious about holding employers accountable, it has to be serious about holding illegal workers accountable. The two aren't separate issues, and they require a strategy with the right tools to deter the use of illegal labor in the workplace.

I urge Congress to push the administration to better delineate how its current worksite enforcement strategy will better maintain the integrity of the U.S. workforce.

Thank you for this opportunity to testify, and I will be happy to answer any questions you might have.

[The statement of Ms. Baker McNeill follows:]

PREPARED STATEMENT OF JENA BAKER MCNEILL

JULY 7, 2011

Chairman McCaul, Ranking Member Keating, and subcommittee Members, thank you for this opportunity to share my thoughts on this very important topic.

I am currently the Senior Policy Analyst for Homeland Security at The Heritage Foundation, a position I have held for over 3 years. In this capacity, I research, write, and speak on homeland security issues, including the issue of worksite enforcement of immigration laws. I should state beforehand that the views expressed in this testimony are my own and should not be construed as any official position of The Heritage Foundation.

Today's hearing will examine the Department of Homeland Security's efforts to protect American jobs and secure the homeland. Specifically, I hope to make three points during my testimony:

- Worksite enforcement of immigration laws is vitally important to our Nation's security, economic well-being, and rule of law. The Obama administration, however, has used its tenure to rollback several key worksite enforcement measures put in place during and prior to the Bush administration.
- The Department of Homeland Security's "employer-focused" strategy for worksite enforcement is inadequate in terms of creating a legal workforce in the United States. It fails to effectively address the problem of off-the-books and identity fraud employment and sends the message that the Government does not take enforcement of our immigration laws seriously.
- An effective worksite enforcement strategy must combat both employers of illegal labor and illegal workers alike, deploying an extensive menu of enforcement tools, meant to combat identity theft/fraud, fake documentation, off-the-books employment, and other abuses of immigration laws in the workplace.

I feel it is important to the discussion of worksite enforcement to first delineate the primary means by which an individual might try to work illegally in the United States. Understanding these illegal methods is essential in terms of assessing the strategies that have been employed by both the Obama and Bush administrations to enforce immigration laws in the workplace. There are three main methods by which most individuals attempt to gain illegal employment:[1]

---

[1] Robert Rector, "Reducing Illegal Immigration Through Employment Verification, Enforcement, and Protection," Heritage Backgrounder No. 2192, October 7. 2008, at *http://www.heritage.org/Research/Reports/2008/10/Reducing-Illegal-Immigration-Through-Employment-Verification-Enforcement-and-Protection* (July 4, 2011).

1. Working "on the books" with a fictitious Social Security number.—In this situation, the illegal worker is employed formally by a business, just as any other employee. The employer withholds Social Security (FICA) taxes and files a W–2 tax form for the employee. The illegal employee presents identity documents to the employer showing that he is either a U.S. citizen or lawful immigrant entitled to work.

These documents will contain a name, date of birth, Social Security number, and possibly a green card number, which are either partially or completely fictitious. The employer dutifully records this fictitious information on an official form called an I–9 and stores the form in a file cabinet. If the information on the I–9 were checked, it would immediately be found to be fraudulent.

2. Working "on the books" through identity fraud.—In this situation, the illegal worker is also employed by a business just like any other employee. The employer withholds Social Security (FICA) taxes and files a W–2 tax form for the employee. The illegal employee presents identity documents to the employer showing that he is either a U.S. citizen or lawful immigrant entitled to work. However, in this case, the name, date of birth, Social Security number, and (in some instances) green card number on the documents corresponds to the identity of a real U.S. citizen or lawful immigrant. To obtain employment, the illegal fraudulently assumes the identity of another real person. The employer records the fraudulent information on the I–9 and keeps the I–9 on file, but neither the employer nor the Government checks to determine whether the employee is the person he purports to be.

3. Working "off the books."—In this situation, the employer deliberately conceals the employment of the illegal worker from the Government. There is no public record of the employee, FICA taxes are not paid, and no W–2 is sent to the Government. It is very unlikely that an I–9 form is completed or kept.

An effective worksite enforcement strategy will deploy enforcement tools aimed at combating all three types of illegal employment.

WEAK ENFORCEMENT HISTORY

The employment of illegal workers has been unlawful in the United States since 1986 when Congress enacted the Immigration Reform and Control Act (IRCA). IRCA set penalties for knowingly hiring illegal workers and sought, through the requirements of the paper I–9 process, to require employers to verify whether newly hired workers could legally work in the United States.

This policy was ineffective at stemming the tide of illegal labor, largely because it was never seriously enforced. While most employers dutifully checked the information given to them from newly hired employees, there was little accountability by the Federal authorities to ensure that employers were following through on their obligations. Furthermore, the Government failed to actually identify and deport those found illegally employed in the United States. Employers had few tools by which to know whether documents and other information provided by employees were fake, authentic, or stolen from another authorized-to-work American or lawful immigrant.

Partially because of this lackadaisical worksite enforcement policy, in the years from 1986 to today, the illegal immigrant population in the United States grew from approximately 2.8 million to 12 million in 2008 and down to around 10.8 million in 2010.[2] Some of this decrease can arguably be attributed to the enforcement measures carried out from 2004–2008 which I will describe below, admittedly however, most of the decrease in the past few years can be attributed to our fledging economy and high unemployment rate which has and continues to discourage many would-be illegal immigrants from choosing to come to the United States. Without a strong enforcement strategy in place, any economic rebound will likely increase these numbers to 2008 levels or possibly higher.

ENFORCEMENT PUSH

From 2004–2008, the Bush administration began an aggressive strategy to ramp-up enforcement of immigration laws in the workplace, including initiatives aimed at both employers of illegal labor and illegal workers alike.

Despite the fact that IRCA provides both civil and criminal penalties to employers that knowingly hire an individual without complying with the employment verification system (the paper I–9 process), prior to the Bush administration, it was

[2] Michael Hoefer, Nancy Rytina, and Bryan C. Baker, Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2009, *http://www.dhs.gov/xlibrary/assets/statistics/publications/ois_ill_pe_2009.pdf* (July 4, 2011).

commonplace that employers found hiring illegal labor might only be subject to administrative hearings and at most civil penalties. The Bush administration, however, began to perform large-scale criminal and civil investigations of employers and used stiff criminal and civil penalties to prosecute those that were abusing the law, while identifying illegal workers.

Popularly referred to as "worksite raids," the Bush administration used unannounced immigration enforcement checks as a means to identify employers of illegal labor and illegal workers. Law enforcement and immigration authorities, pursuant to a criminal investigation would arrive unannounced at workplaces suspected of employing illegal immigrants and require proof of legal status. The employees found to be illegal would be turned over to law enforcement, while employers would be subjected to fines and other penalties for employing illegal labor. These checks were essential in terms of discovering all three types of illegal employment and served as a huge deterrent mechanism to those seeking to avoid the law.

Other efforts used by the Bush administration included the expanded use and promotion of E-Verify—an on-line tool by which to check the employment status of newly hired employees. While deployed on a limited basis as a pilot program since 1996, it was extended to all 50 States in 2003. E-Verify today remains a voluntary program, and yet has more than 225,000 participating employers.[3] As part of the Bush administration's push to increase participation in E-Verify, the administration propagated a rule, in place today, which requires all Federal contractors to use E-Verify for their employees.

The Bush administration also began an effort in 2007 to use Social Security No-Match letters as a worksite enforcement tool. The Social Security Administration (SSA) has long issued letters to workers to let them know that there was discrepancies in the use of their Social Security numbers. In 1994, the SSA began sending such letters to employers with 10 or more no-match W–2 forms. The Bush administration, however, issued a new rule clarifying that receipt of such a no-match letter "may," depending on the circumstances, constitute constructive knowledge that a worker is unauthorized. The rule then granted employers a safe harbor from immigration enforcement actions based on no-match letters when they took certain simple actions, such as double-checking their records.[4] After a court challenge, DHS proposed a supplemental rule which would have resolved court concerns over the rule's implementation and yet still preserve No-Match as an enforcement tool. However, the administration was unable to follow through with full implementation before the end of its tenure, and the Obama administration would later completely abandon the effort.

When the Bush administration began actually enforcing immigration laws in the workplace, the frequency of worksite arrests jumped from 845 in fiscal year 2004 to 6,287 in fiscal year 2008. These efforts were essential first steps towards effectively identifying individuals working illegally in the United States and employers that were abusing immigration laws. While certainly not the end of the road for worksite enforcement, augmented and effectively deployed, these efforts did and would have continued to have a gigantic impact on worksite enforcement.

"CHANGE" IN STRATEGY

The Obama administration, upon taking office, announced a change of course in terms of its own worksite enforcement strategy. It has emphasized that it has switched to one that is "employer," rather than "employee" focused, taking the emphasis off of identifying illegal workers, and more on punishing those who hire illegal labor. What this has meant in practice, however, seems to be significantly less worksite enforcement than the Bush administration.

For instance, the administration has emphasized that it no longer prefers to use "worksite raids" or unannounced worksite enforcement checks, largely abandoning criminal investigations in favor of civil actions. Instead, it has focused its efforts on paper I–9 audits where employers would be told in advance that they will be audited and are given significant lead time by which to clear out a staff of illegal labor. Even upon auditing, employers are largely left free of additional investigation as long as they are filling out the I–9 paperwork appropriately. Essentially, with plenty of notice, it is fairly easy for most employers to clean-up their payroll to pass the

---

[3] United States Citizenship and Immigration Services, What is E-Verify? *http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=e94888e60a405110VgnVCM1000004718190aRCRD&vgnextchannel=e94888e60a405110VgnVCM1000004718190aRCRD* (July 4, 2011).

[4] Charles Stimson and Andrew Grossman, No Match Immigration Enforcement: Time for Action, Heritage *Legal Memorandum* No. 25, at *http://www.heritage.org/Research/Reports/2008/05/No-Match-Immigration-Enforcement-Time-for-Action* (July 7, 2011).

Obama administration's muster. While these audits look nice on paper, they do very little in terms of actually enforcing immigration laws.

In at least one instance where the Department of Homeland Security has performed investigations into employers, the enforcement check reportedly resulted in no identification, detention, or deportations of apprehended illegal workers. In February of 2009, an investigation into Yamato Engine Specialists Company in Bellingham, Washington yielded 28 illegal workers. The Secretary of Homeland Security, however, apparently uninformed of the enforcement check, according to press reports, gave the apprehended workers temporary work permits.

This pattern sends a message that the administration is not serious about enforcement. But it is also disappointing because the actual apprehension of illegal workers was often helpful to investigators during the Bush administration as witnesses to provide testimony in a prosecution of employers for abuse of the law.

Rescission of Social Security No-Match.—Instead of pushing forward with the supplementary rule propagated by the Bush administration that would have likely met court muster and allowed for full deployment of no-match as an enforcement tool, the Obama administration halted no-match letter issuance completely and expressly emphasized its intention to prevent the use of such letters as evidence for constructive knowledge of unauthorized workers. While the administration has in recent months quietly begun issuing letters again, it has shown no appetite to push forward with the Bush administration's plan to use no-match as an enforcement tool. Given that the administration has emphasized its preference for an "employer-focused" strategy for immigration enforcement—such a policy should fit squarely into the administration's agenda.

Abandonment of REAL ID.—REAL ID was enacted in 2005 in direct response to the 9/11 Commission Recommendation that the Federal Government set secure standards for identification as a means of preventing terrorist travel, but also to combat identity theft and fraud. Given that identity theft and fraud is one of the biggest challenges facing worksite enforcement and driver's licenses are routinely used as part of the worker verification process, requiring States to meet a minimum standard for driver's licenses only makes sense. However, while many States have moved forward to meet the Act's requirements, the administration has spent more time trying to get the Act repealed or replaced than meeting implementation deadlines. The administration's efforts to get rid of the mandate make little sense if it is serious about combating the rampant identity theft used to obtain employment illegally.

At the same time as rolling back these measures, the Obama administration has made E-Verify the centerpiece of its worksite enforcement strategy and has pushed aggressively to increase participation in the E-Verify program. At a conference on E-Verify in 2009, Secretary Napolitano stated that "E-Verify is at the centerpiece of our efforts to maintain a legal workforce both for large and small businesses."

Let me emphasize, E-Verify is an outstanding tool for catching the use of fake information by would-be illegal workers. It can accurately and inexpensively do so and it absolutely should be promoted. However, it is not a silver bullet solution for enforcement and should not be sold as such by the administration. For instance, E-Verify cannot catch off the books employment. It also does not catch situations where an illegal worker steals a legitimate Social Security number and other documentation and gives that information to an employer. In essence, without other tools aimed at squeezing out other forms of illegal employment, an E-Verify focused enforcement strategy will simply further the market for identity theft and off-the-books employment, and only detect a small percentage of the illegal workforce.

AN EFFECTIVE STRATEGY

The Department of Homeland Security's so-called employer-focused strategy has resulted in less enforcement, not more. While it has in some instances exceeded the Bush administration's levels in terms of sheer number of investigations and penalties, these efforts have largely lacked in substance, and have done very little to actual stop the employment of illegal labor. Some of the right questions to be asked should be the number of worksite arrests, what actions ICE has taken to investigate identity theft discovered in the course of an investigation, and what steps is it taking to follow up with employers that have been investigated through a soft I–9 audit.

If DHS is serious about holding employers accountable, it must also be serious about holding illegal workers accountable. The two are not separate issues, and require a comprehensive strategy aimed at disincentivizing the use of illegal labor in the workplace.

Effective enforcement requires a menu of enforcement tools aimed at squeezing all forms of illegal labor out of the market, including off-the-books, identity theft, and fake documentation. Such a menu of enforcement tools should include:

- *Reinstatement of worksite enforcement checks*.—These checks, pursuant to a criminal investigation are a valuable tool in terms of identifying those employers that are consistently hiring illegal labor. Diluting their effectiveness by alerting employers or not actually identifying, detaining, and deporting identified illegal workers makes such raids useless.
- *Continued use of civil audits in conjunction with criminal enforcement*.—I–9 audits can be used effectively to alert employers of potential violations of immigration law. These audits should continued to be used, in conjunction with a robust criminal investigation process. Together, these actions can provide the deterrent effect necessary to combat violations of worksite immigration laws.
- *Provide resources to limit the impact of worksite raids on families and local communities*.—While worksite enforcement checks are a perfectly legitimate and effective means by which to identify illegal workers, the impact of these raids on families and local communities should not be ignored. Often the children of detainees, most of them U.S.-born citizens, suffer when their parents are detained and deported. ICE has tried to put in place several initiatives to allow families to stay together during the deportation process as well as the release of sole caregivers from detention facilities. The Obama administration could go further to coordinate with local communities before and after raids, including working with schools, social services, and religious institutions to ensure that no children are being left behind, as well as working to ensure quick release of sole caregivers to minimize the time that children of single parents are left in the care of others.
- *Continued efforts to promote and improve upon E-Verify*.—E-Verify is highly accurate at detecting false information provided by an illegal worker. It should continue to be promoted as a means for employers to check the work eligibility of their employees. Congress and the administration should remain committed to its reauthorization and to continually refine the accuracy of its databases. Another step may be to investigate whether employers are actually discharging the employees who receive final non-confirmations.
- *Promote IMAGE*.—IMAGE is the ICE Mutual Agreement between Government and Employees. It was meant to improve internal enforcement by giving companies training on ICE on hiring procedures, detecting fraudulent documents and using E-Verify. In addition, participating companies have to undergo an I–9 audit and check the legitimacy of existing employees' Social Security numbers. IMAGE should be supported in order to give willing companies more resources by which to ensure the legality of their workplace.
- *Move forward with Social Security No-Match as an enforcement tool*.—No-Match has the ability to help tackle identity theft situations and help employers identify illegal workers in their labor force. A next step would be to allow information sharing between DHS and SSA on no-match data to assist in immigration investigations.
- *Examine supplemental procedures to prevent identity fraud/theft*.—One method may be for the SSA to scan its wage database to identify individuals who held two or more jobs at the same time, over an extended period, were receiving Social Security benefits, or were employed under the age of 16. These red flags could then be used by SSA to send a letter to the individual notifying them that a potential identity theft may have occurred.
- *Ramp-up support for investigations of off-the-books employment*.—While off-the-books employment situations are the most difficult for investigators to tackle, additional resources for investigations of these incidents could decrease the incentive for employers to hire workers in this manner.
- *Increase penalties for unlawful hiring*.—The financial penalties for hiring legal workers is too low, so low, in fact that it does not always deter illegal hiring. As a result, many employers can factor in fines as a cost of doing business. Congress should look to set fines in a way that will have an actual deterrent effect.
- *Move Forward with REAL ID*.—Postponing or modifying implementation confuses the work already in process and detracts from the underlying purpose of REAL ID—to maintain security and combat identity theft.

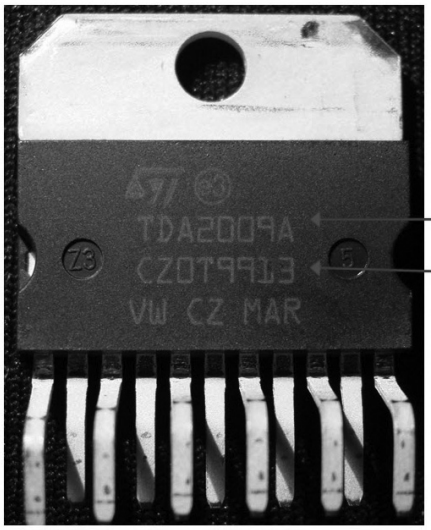
A legal workforce is absolutely essential in terms of an effective immigration strategy that preserves National security, promotes the economy, and maintains rule of law. I urge Congress to push the administration to better delineate how its worksite enforcement strategy will meet these goals.

Thank you for this opportunity to testify. I would be happy to answer any questions you have at this time.

Mr. MCCAUL. I want to thank the witnesses for their testimony. The Chairman now recognizes himself for 5 minutes.

Mr. Toohey, I want to start with you. We have some photographs I hope we can put up on the screen that deal with the issue you were talking about. As I understand it, this is a semiconductor chip that has included information about date and manufacturing location codes; is that correct?

[The information follows:]



Mr. TOOHEY. That is correct, Mr. Chairman.

Mr. MCCAUL. Why is that important?

Mr. TOOHEY. It is important because in this context it enables us to determine whether or not the chip is authentic or counterfeit. Companies have databases which can tell you exactly where the chip was manufactured, on what day, what type of chip it is, and by verifying the type of chip versus that coding system, we can almost instantaneously verify whether that is an authentic chip or not.

Mr. MCCAUL. Okay. So DHS would come to you and say, hey, we have got this chip, is this authentic, is it yours, and if it is not, if it is counterfeit, they need to confiscate it, correct?

Mr. TOOHEY. Yes, sir.

Mr. MCCAUL. That was going on between—that was the practice——

Mr. TOOHEY. Practice for many years.

Mr. MCCAUL. Two-thousand to 2008 or——

Mr. TOOHEY. Even before, Mr. Chairman—sorry. Even before 2000, it was the practice for many years. Starting in 2000, they stopped sending out the actual product and just sent us pictures, which is fine. As long as we have the code, we can determine. Actually it was a system that worked very well, but in 2008 it all stopped, and they redacted the information from the pictures that they were sending.

Mr. MCCAUL. So early on they would actually send you the actual product, which is the best evidence, then they sent the picture which had information on it so you could identify, and then in 2008 something else—something happened—and let us show the other picture if we can. This is what you get. Is this an example of what you would currently receive from DHS?

[The information follows:]

Mr. TOOHEY. Yes, Mr. Chairman, and as you can see, it is virtually impossible—you can't see the number, and it is virtually impossible based on that for anyone to authenticate that chip.

Mr. MCCAUL. You don't have the trace codes or any of the information contained in the previous photograph to identify this intellectual property, this semiconductor chip?

Mr. TOOHEY. Yes, Mr. Chairman, that is exactly right.

Mr. MCCAUL. It is astounding. Why? Has DHS explained to you why they have stopped providing this kind of information?

Mr. TOOHEY. Yes. First of all, let me clarify. This isn't a policy that was directed only at our industry. It affects all products, and it was based on a reinterpretation that Treasury Department, which has policy responsibilities in this area, established in 2000. It was a reinterpretation of the Trade Secrets Act, in which it determined that—or at least its opinion was that by sending that information to the manufacturer, that would violate the disclosure of confidential information provisions of the Trade Secrets Act.

As I mentioned in my statement, that just doesn't make any sense, even common sense, because to the extent anyone owns that publicly viewable information, it is the manufacturing. It is the company that it would be sent to. We provided detailed legal anal-

ysis to the Department of Treasury and DHS in terms of why that just isn't the case. They haven't really given us any reason why our legal analysis is wrong.

Part of the motivation that I understand is a desire to protect parallel importers, so as to not have any, you know, information disclosed to manufacturers that could affect importers, but there is nothing in that code that can tell us who the importer is. At the most it could tell us who we originally sold it to, but that information simply is not possible to obtain from that code. So, from our perspective, that doesn't make much sense.

You know, if one can even understand that justification for handbags or some other products, you know, one could maybe understand it, but for products where there is critical, you know, life-saving technologies, health and safety, our soldiers' technologies on the line—we know for a fact, as you said in your opening statement, Mr. Chairman, this is a clear and present danger. We know that there is 15 percent of current inventories of the Pentagon where these chips are counterfeit. So we know this is a problem. We know that this is an on-going issue, and it is affecting the lives of our soldiers and the health and safety of our citizens. So, in this particular area, it just doesn't make any sense to us why we would tie our hands and not allow our industry to help the Government determine instantly where these products are coming from.

Mr. MCCAUL. You want to help the Government identify counterfeit chips, and it is my understanding the lawyers at the Department have now determined that they cannot give you this information unless they have basically, you know, taken all the identifying information off of it. How can you possibly identify something as counterfeit when they have taken off all the code numbers?

Mr. TOOHEY. You are exactly right; you can't, Mr. Chairman.

Mr. MCCAUL. You can't?

Mr. TOOHEY. You cannot.

Mr. MCCAUL. So, as a result of this legal policy or analysis that was done, we probably have God knows how many counterfeit chips coming into this country, and we are excluding the private sector from being able to assist DHS in identifying, you know, counterfeit chips coming into the country; is that correct?

Mr. TOOHEY. That is exactly correct, Mr. Chairman. We are desperate to help. We have been begging Treasury and DHS to let us help stop dangerous chips that are coming in.

Mr. MCCAUL. Well, we are going to try to help you. I hope Mr. Thompson—I don't see this as a Republican or Democrat issue. I see it as just a common-sense issue that I hope perhaps we can work together to change this policy. Otherwise we are going to have counterfeit goods coming in that can't be identified.

I want to try to hit a quick question with each of you. I know my time is limited, but going to Mr. Russo, you know, I talked about the example of just one drug going to so many different countries around the world and finally ending up in the United States being counterfeit. When we talk about this chain of supply, what do you consider to be the greatest threat to pharmaceutical companies, the supply chain?

Mr. RUSSO. Mr. Chairman, the greatest threat that we see to the supply chain is what is available over the internet. The ease in

which a consumer, wherever it is in the world, can order counterfeit pharmaceuticals over rogue websites presents a significant threat to patients in the United States and, for that matter, other countries.

Mr. MCCAUL. You know, there has been some talk about making it legal for people to import from Mexico and Canada. Does that pose any threat in terms of the quality of the product?

Mr. RUSSO. The problem is that when you look at internet sites that sell pharmaceutical products, what you look at is what is a very slickly designed website with a person in a white coat with a stethoscope around their neck, and the patient throws a credit card in there and orders product, and you really don't know what you are going to get. You could get diverted product, you could get stolen product, you could get counterfeit product. As you said in your remarks, sir, those products are less than efficacious and don't treat disease. So that is the issue is you have a slick front, and you don't know what is behind that, and as we have purchased from those sites, we found many of those products to be substandard coming into the United States.

Mr. MCCAUL. Do you know what percentage of these consumers are seniors that buy their medications on-line?

Mr. RUSSO. No, Mr. Chairman, I don't have that data. We see a lot of different consumers buying over the internet, you know, for various reasons.

Mr. MCCAUL. If I can move on to Mr. Mancuso, you know, in my prior life I worked at the Department of Justice. We worked quite a bit on Export Control Act cases, dual-use technologies, so I am very familiar with that. Most of these cases involved China, you know, and we know that the most probably hacked-into office from a cyberattack is this export control office within the Department of Commerce, for obvious reasons.

What more needs to be done to protect—you know, we don't want to slow commerce down, but we certainly don't want to be giving nations, you know, that don't have our best interests at heart, you know, technology like the example I gave; one is it is a medical device, but that it can be used, you know, for a nuclear device. What more needs to be done?

Mr. MANCUSO. Mr. Chairman, I would suggest, just to begin with, to distinguish two things. First is refining our export controls and reaching out to industry to ensure that the private sector is really a partner in enforcement. You know, many U.S. companies want to help and have more information at their disposal with respect to industry competitors who may not be complying with the law.

On the other hand is industrial espionage, which is, of course, different because industrial espionage is the intentional theft of technology. I think we have to, specifically with respect to State-based competitors, near-peer competitors, looming adversaries perhaps, we need to buttress our counterintelligence capabilities to figure out what technologies they are interested in and what vectors they use to acquire our technologies.

So I would submit to you, Mr. Chairman, that there are two things: Export controls and outreach to industries to ensure that on the U.S. side of the equation, industry knows what is controlled,

how it is controlled, how it can be exported. But on the sort of foreign side, we need to build a better firewall in terms of our counterintelligence capability to uncover, prosecute industrial espionage.

Mr. MCCAUL. Thank you.

Last question to Ms. McNeill on the worksite enforcement issue.

According to the Congressional Research Service, since this administration has come into power, administrative arrests have declined 77 percent, criminal arrests have declined 59 percent, and convictions declined 66 percent. I know there was a shift in policy in terms of going after, I guess, employers and not the employees, but these numbers are, to me, very disturbing in the sense that we are not enforcing the law. What is your opinion?

Ms. BAKER MCNEILL. Well, you know, it is sometimes very difficult, Mr. Chairman, to disaggregate the employers of illegal labor from the illegal workers. You know, if you look at the situations where they—if they are in the Bush administration, during worksite arrests they may find individuals who either the employers had knowledge of the identity theft ring that was going on, that the employers maybe were violating other workplace standards, other immigration laws in the workplace, and these illegal workers were so essential to providing that kind of case to be able to prosecute employers. So you can't take one and not have the other to have an effective enforcement strategy. You really have to do both because they work—you know, they work off of one another. It is an economic problem because workers want jobs, employers need labor. So we have to attack it from both sides.

Mr. MCCAUL. This hearing is really about protecting intellectual property and innovation in this country and protecting American jobs, jobs that Americans would have but they're losing. So, you know, the E-Verify I always thought has great promise if it is fully implemented. The verification on Social Security numbers, if we could fully implement that. But we just have never—and I'll say in fairness to both the prior administration and this administration, we have yet to fully implement that program.

Ms. BAKER MCNEILL. Well, I will give significant credit, Mr. Chairman, to the Obama administration for taking the time to look at ways to improve E-Verify as a system. They have done E-Verify self-check, which essentially allows individuals to go and look at their own information. That only helps improve the accuracy of E-Verify. So I think that is an area. But we can't make E-Verify the only centerpiece enforcement tool, because it doesn't take into account identity theft and off-the-books employment, which are huge issues in the workplace.

Mr. MCCAUL. Thank you.

My time has expired. The Chairman now recognizes the Ranking Member of the full committee, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Since we are talking about American jobs and how this process yields some increased numbers, Mr. Toohey, I looked at your semiconductor picture, and it struck me that most of the problems we are dealing with is these chips are made somewhere else. If we really wanted to generate some jobs, I would think we would try to bring that business back here. Has your industry ever looked at

what it would take to bring that industry back, thus creating new jobs and eliminating a large portion of this counterfeiting that's going on right now?

Mr. TOOHEY. Well, thank you, Mr. Ranking Member.

Our industry is committed to building jobs in this country. As I mentioned in my opening statement, we manufacture the majority, about 75 percent, of the chips that we sell all around the world here in the United States. So we are very much committed to manufacturing and design here in the United States, and it is something that we continue to build and we continue to invest in manufacturing here in the United States.

This counterfeit problem is a little bit different. Most of the chips that come back as counterfeits were originally manufactured as some other type of chip, probably here in the United States, and they're sent around the world as e-waste, you know, old computers, old things.

The counterfeiters, they don't have the capability to manufacture chips themselves. They can't build $5 billion fabrication facilities. They take these old chips out of old computers or old cell phones and then they remark them as something, you know, milspec chips or some very specific application, and then sell them as international brokers.

So the problem is it is not that they are manufactured overseas originally or that there is great investment in jobs. That is mostly still here, Mr. Ranking Member. The problem is that these counterfeiters then take the waste and then mark them up and then send them back here as something else, and that's what we need to stop.

Mr. THOMPSON. So have you looked at or has your trade group looked at any additional methods that it would recommend to prevent those chips from coming back in?

Mr. TOOHEY. Thank you, Mr. Ranking Member.

Certainly closing the front door, taking the very discrete action that we recommend would be an enormous help, something we could do today that would significantly advance our efforts and prevent these counterfeit, dangerous chips from coming in. So that's one aspect.

Another aspect is increasing the prosecution of these unscrupulous dealers. Much of the prosecution—and ICE and other agencies are great at doing this, but providing—stopping the counterfeiters first will actually facilitate additional prosecutions.

From the Business Week articles and others, you will see that many of the dealers selling chips into the DOD system are these small, unscrupulous dealers. They know what their problem is.

A third area where I think we could do more is in tightening up our Federal acquisition regulations so that DOD, DHS, other agencies only purchase from authorized dealers. That's not the case today. That's something we ought to look at.

A final area, Mr. Ranking Member, is working with our international partners more closely. We know where these chips are being counterfeited. We know they're being sold openly in Shinsen in a big market there. One of my colleagues just came back from there and brought some samples he was freely given. We know exactly where this is, and so we need to work more closely with China to stop this and increase enforcement on the ground.

Those are some other practical measures we could take.

Mr. THOMPSON. Thank you very much.

Mr. Russo, with respect to counterfeit pharmaceuticals, I think part of your testimony talked about these rogue websites and the fact that a number of them have been shut down, but a number of them still exist. Taking off from the Chairman's comments, sometimes people are lured to those sites because of the cost factor of the drugs. A lot of seniors get caught up in the trap. Knowing that a disproportionate number of those individuals might be seniors, has your industry looked at any programs that could drive seniors back to the marketplace versus the websites?

Mr. RUSSO. Thank you, Mr. Ranking Member.

I want to say that no pharmaceutical company wants to see a patient that needs medication without product. To help seniors and others who don't have funds to buy product, there are a number of programs that our company has and other competitors to us have for seniors who can't afford medication. Many of those are available publicly on our website. Through some of the enhancements in Medicaid and Medicare, there are other programs for seniors. So there are, we believe, a number of ways for seniors who don't have funds to obtain product; and we encourage them to use those programs to seek safe and efficacious pharmaceutical products.

Mr. THOMPSON. I appreciate your indulgence, Mr. Chairman.

You know, we created the position of Intellectual Property Enforcement Coordinator; and to the extent that that's been there for a while, Mr. Toohey, can you comment as to what the industry's experience has been with that operation?

Mr. TOOHEY. Sure, I would be happy to. Thank you, Mr. Ranking Member.

We have had a great experience with Victoria Espinel and her office that has been tremendously helpful to us in a wide range of areas in intellectual property enforcement globally. So that office, as a matter of fact, used—they spent a lot of time trying to help us solve this problem, but they weren't able to change the Treasury Department's and DHS' policy views. They weren't able to overrule them. But we have had a fantastic experience and great support from that office.

Mr. THOMPSON. What about you, Mr. Russo? Do you have any contact with that office?

Mr. RUSSO. Thank you, Mr. Ranking Member.

I would echo Mr. Toohey's comments and say that I personally have been very impressed with Ms. Espinel and her staff who have really got to the low-level understanding of the issues that face our industry and, as you can see, their industry; and they have been very helpful and very effective in helping us fight counterfeit pharmaceuticals.

Mr. THOMPSON. Thank you.

I yield back, Mr. Chairman.

Mr. MCCAUL. I thank the Ranking Member.

The Chairman now recognizes the gentleman from Missouri, Mr. Long.

Mr. LONG. Thank you, Mr. Chairman.

Mr. Toohey, you testified that we need to take proven, common-sense steps, which the trouble with common sense is it isn't common, as you know.

Then you said that 15 percent of—was it—spare chips purchased by Department of Defense are counterfeit.

Now I have got a visual in my head of a guy in a trench coat standing over at the Pentagon saying, hey, buddy, you want to buy a chip? How in the world are we buying 15 percent of counterfeit chips? What's the supply chain? Where do those come from?

Mr. TOOHEY. Well, Mr. Long, thank you very much for the question.

It is a big problem that we would recommend be fixed, and the Department of Defense and the Federal acquisition regulations need to be tightened to only purchase through authorized dealers. Right now, they purchase essentially at the lowest price. The regulations are the lowest price. Anybody who is willing to sell them these chips or other military products is, at least my understanding, they have to purchase at the lowest price. So they purchase, many times, from these very kind of fly-by-night, unscrupulous dealers who get their chips from China; and they mark them up as milspec and——

Mr. LONG. Educate me. What is milspec?

Mr. TOOHEY. Sorry. Military specifications, so increased heat and endurance, you know, very sophisticated equipment.

So, you know, it is—that system is broken. So part of the solution would be to tighten our Federal acquisition regulations, especially for the critical areas like DOD and DHS, to make sure they are only buying from authorized dealers. That just makes sense. That's just in our National interest.

So we would strongly recommend—we have been recommending for many years—that the Department of Defense do that.

Mr. LONG. These are coming in large enough quantity—obviously, they are—where they can buy 15 percent of them.

Mr. TOOHEY. Yeah. That's their number. Officials publicly have said that from DOD and said that's what they estimate.

Mr. LONG. On your first exhibit, which was the authentic and the counterfeit voltage regulator and automotive airbag brake systems, the numbers on there, they don't look to be quite identical. But walk me through the redacted part where they are sending you these redacted pictures. What are those pictures of? Are these shipments that they suspect are counterfeit or they know are counterfeit and then they send the industry these pictures with the redacted information?

Mr. TOOHEY. Yes, Mr. Long. They are suspected counterfeit. So for whatever reason, maybe it is the location they came from, the way they are packaged, the port officers suspects that they don't look quite right. So, in that instance, they traditionally send us the full picture of the chip where we can tell them right away whether it was authentic or not.

Mr. LONG. How can you do that? It looks like they could copy identical the coding and everything if they're going to—I mean, that's what I am having trouble with is understanding how that helps you. Because it looks to me like they could—if they are going

to counterfeit the chip, it looks like they could counterfeit the identifying numbers.

Mr. TOOHEY. Well, they don't always have the exact type of chip that they are trying—many times, they are selling very sophisticated, advanced chips, and what they are dealing with are those old e-waste, and so they take numbers that——

Mr. LONG. Is that 100 percent of the time this all starts with e-waste?

Mr. TOOHEY. Mainly, yes. I mean, almost always. They don't manufacture their own chips, so they get them from some other place.

Mr. LONG. I am flabbergasted that there is that much volume out there where they could, all through e-waste, and come up with a big enough shipment to ship to our military and we are buying 15 percent of counterfeit product. It is just mind-boggling.

Mr. TOOHEY. Yes, sir, it is. It is a system that we can dramatically improve today by making the right type of policy change.

Mr. LONG. Okay. I hope we can help you with that.

Mr. TOOHEY. Thank you, Mr. Long.

Mr. LONG. Mr. Russo, are you aware of any instances where a country has prohibited FDA to inspect a facility within that country?

Mr. RUSSO. Thank you, Mr. Long.

That's an area of expertise I don't have. My remit is strictly counterfeit. FDA inspects a lot of facilities for compliance and regulatory matters, and it would not be information that I have. But I would be happy to go back to my company, to the experts in that area, and get you a written response.

Mr. LONG. If you would, I'd appreciate it. Also to follow up with the written response.

If there are countries that are doing that, my next question would be if you all have any facilities within those countries.

Mr. RUSSO. Yes, sir. We will follow up, and I thank you for the question.

Mr. LONG. Thank you, Mr. Chairman. I yield back.

Mr. MCCAUL. Thank you, Mr. Long, for your questions.

We are going to follow up on this issue. It is unacceptable that 15 percent of the military's semiconductor chips are coming—well, not only foreign countries but counterfeit. So I think that's going to be one of the tangible takeaways we will get from this hearing, and I appreciate your help on that.

The Chairman now recognizes the gentleman from South Carolina, Mr. Duncan.

Mr. DUNCAN. Thank you, Mr. Chairman.

You know, sitting here, thinking about it, just listening to the testimony, I think it is ironic that we are debating a defense authorization or appropriations bill this week when so much money has been spent with independent contractors out there that are supplying these chips.

I want to reference a *Business Week* article. The cover says "Dangerous Fakes", and the article talks about a contractor out in Bakersfield, California, who wasn't involved in any sort of microchip business before, but she heard there may be a business opportunity to begin selling microchips to the military. So she created a busi-

ness in her home, and since 2004 she has won Pentagon contracts worth a total of $2.7 million. The military has acquired microchips and other parts from her for use in radar on the aircraft carrier Ronald Reagan and antisubmarine combat systems of destroyers. She said she knows very little about the parts that she buys.

So I am sitting here thinking about all the money that we spend with these independent contractors that, if you look at what she went through to get that military contract, it was very little. Then, to find the products that she sells, she plugged parts into Google—part codes into Google and found websites offering low prices. She bought those microchips from the website and sold them to the military.

So I'm sitting here thinking how many men and women in our armed services are in harm's way because of faulty microchips that might be in an airplane system, now that we are doing fly by wire in the F–18 and other future aircraft. How many faulty weapon systems or faulty chips are in weapons systems there in the drones that are used and in commercial aircraft? I'm going to take this even further, commercial energy production, nuclear power, the power grid?

We know what happened in Iran with the centrifuges with the virus that shut them down. Do any of these microchips—is there a possibility of espionage from a country or a rogue entity that puts a virus in place or puts a back-door access code that they can access these power systems on the commercial side, not on the military side?

So these are things that I'm thinking about. So my question to you is: Where are most of these microchips being produced? What countries would you say they are coming from mostly?

Mr. TOOHEY. By far, China. By far some specific places within China, that they take the old, used electronics and take out the chips and then, you know, sand off the number and put a new number on and then repackage them, sell them to people like the person you mentioned, very unscrupulous dealers. Unfortunately, that's not an isolated incident. But we know exactly where they are coming from.

These are counterfeit chips. Just a couple of days ago one of my colleagues was there in Shinsen and walked openly in the market. He was given samples of counterfeit chips. So we know exactly where it is. You know, part of the solution is certainly targeting those places.

But I think the first thing we ought to do is use the very practical, known, proven solutions to close our front door. There is, obviously, a multi-tiered effort. We have to go on tightening up our Federal acquisition regulations, prosecuting these people, these unscrupulous dealers, and working with other countries, especially China.

Mr. DUNCAN. What other countries are better to work with than others? Do we have some that are proven difficult to work with?

Mr. TOOHEY. Well, I think China has been difficult to work with. I think our Government officials would tell you, on overall enforcement of intellectual property, there are efforts certainly going on in China to step that up, which we appreciate, but we need more, and

we need a stronger focus on the part of our trade negotiators. But this problem almost entirely emanates from China.

Mr. DUNCAN. Mr. Chairman, I am concerned that DHS is writing security directives that change policy without Congressional authority and Congressional consent and holding up the ability to verify the validity of these chips that are coming in. Through digital photography and email, it can be almost instantaneous; and I appreciate the companies that are willing to work with the DHS in trying to solve this issue.

We had an issue of a carburetor on a small engine that—EPA requires an anti-tamper or adjustment mechanism on the carburetor so that you can't adjust the carburetor and emit more pollutants into the air. So these came into a port. Homeland Security and CBP held that shipment up. A member of the Customs and Border Patrol was able to defeat the mechanism that blocked that device and that blocked your ability to adjust that carburetor over a period of an hour with a hammer and a screwdriver. They held up that whole shipment, even thought that blocking device was approved by the EPA prior to this.

But yet the Department of Homeland Security will not simply take a digital photo and send it to a company who is willing to say that is our chip or not our chip. We have got our priorities mixed up in this country, especially when it comes to espionage or for our power grid and protecting our armed services, the men and women defending our liberties in this country, and we are failing to do that, and these chips are going into weapons systems and into our commercial power grid.

This is a very timely meeting, Mr. Chairman. I appreciate that. Thanks, guys, for coming.

Mr. MCCAUL. Thank you, the gentleman from South Carolina, for your remarks.

I think the Chinese have a saying, why invent it when you can steal it? So that's what they do. There is no incentive. They steal our intellectual property. They engage in espionage. They hack our systems, every Federal agency, and now we have our own department tying our hands with the private sector to be able to identify what's counterfeit.

We will take action, and that's what this committee is all about.

With that, I recognize the gentleman from Alabama, Mr. Rogers.

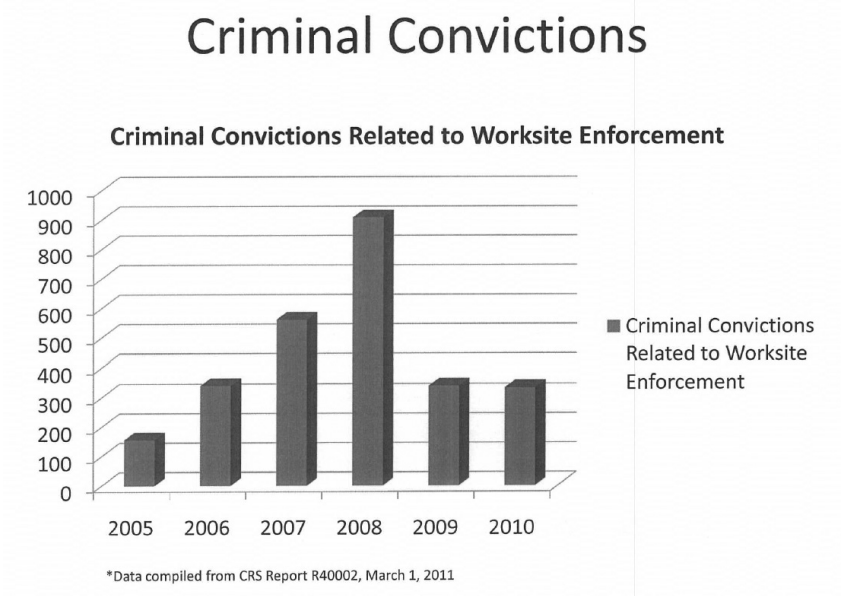
Mr. ROGERS. Thank you, Mr. Chairman.

I listened to your opening statements, yours and the Ranking Member's, and they're pretty different. You paint a pretty grim picture of ICE's effectiveness in the last 2 years and the statistics, and then the Ranking Member comes back with statistics that makes it appear that the Obama administration, through its ICE director, has just been doing a stellar job. I am really confused about which of those is correct. I have asked my staff to get both of your statements and look at the supporting evidence so we can find out which is right.

But I can tell you my personal experience is John Morton and ICE have decided not to pursue worksite enforcement and not enforce the law. I think the best evidence of that, aside from the statistics, is his own employees gave him a vote of no confidence for refusing to allow them to enforce the law.

I have got a chart up on the board right now that states—and this is from CRS. This is not my numbers, CRS showing the number of criminal convictions in the last 2 years. You can see the last year of the Bush administration we had a very high rate. My guess is, as a recovering attorney, that most of the 2009, 2010 cases were in the pipeline when this administration took office. I would be very interested and will be interested in seeing what 2011 and 2012 look like.

[The information follows:]



Mr. ROGERS. But I want to talk—this is less for Mr. Toomey and Russo than it is for Mancuso and McNeill. I have got a problem in the south in that we have a lot of illegals working for companies just to be more competitive. We have turned in—I know of companies that have turned it in to ICE, and I have turned them in, just to find ICE not to do anything about it. This has basically been the stated position since this administration came in, that they were going to cease worksite raids or dramatically reduce them. First, it was because of the census. We didn't want to chill the enthusiasm of illegals being counted. You know, then it was, after that, well, it's because we don't want them to be afraid of the police or reporting robbery or whatever. But it's always an excuse as to why we don't want to alienate the illegal Hispanics that are here in the country and punish their employers.

I notice in Ms. McNeill's statement that you talk about the administrative change, getting away from, even using the phrase "worksite raids". Tell me more about that.

Ms. BAKER MCNEILL. Mr. Rogers, as far as—are you asking specifically about my use of the phrase?

Mr. ROGERS. No. You talk about the fact that this administration made a conscious decision to move away from worksite raids. Why? What's their stated reason?

Ms. BAKER MCNEILL. Well, there has been a number of stated reasons. Partially, it has been because they have said that it is better to go after employers because employers were the ones hiring the illegal laborer and that the illegal workers were simply just taking jobs.

Mr. ROGERS. Have they followed that up with actual raids of work sites and criminal actions against employers?

Ms. BAKER MCNEILL. My impression is it is kind of twofold. The first is that there have been a few investigations that have occurred. I won't say that that didn't happen ever. There have been some worksite raids. But in those cases you have had the fact that the illegal workers were oftentimes not even identified, much less detained or deported. They weren't even identified. These could be significant rings of identity theft that we just kind of let them go or give them temporary work permits.

On the other side, you have the fact that, while criminal arrests under the Obama administration of employers are up, that that statistic is there, the reality is that, for most employers, they have been sent the message that they are only going to be subject to a civil I–9 audit.

Mr. ROGERS. So that arrest is going to arise in a civil penalty rather than a criminal penalty.

Ms. BAKER MCNEILL. Well, somewhat. For most of the employers who were doing the kind of on-the-books employment, they have been sent the message, because they are only being subject to I–9 audits and not really criminal investigations, that what they will get is their notice that they are going to be audited and, you know, they get a decent amount of time by which to basically clear their rolls of people that they think are suspicious.

Mr. ROGERS. So what happens with the arrest? I am trying to figure out where the arrest comes in.

Ms. BAKER MCNEILL. Well, from what I know, the Obama administration has done some smaller investigations of employers where they have done arrests. But as far as from what I have seen, as far as big employers who have lots of labor and potentially lots of illegal labor, they are not even touching them with criminal investigations.

Mr. ROGERS. Mr. Mancuso, do you agree with that?

Mr. MANCUSO. I generally do agree with that.

I would also add that in our setting, in the export control sort of enforcement setting, it is actually even a more fundamental problem. If someone is inside the country illegally, it stands to reason they are in the country illegally. That's a problem.

But even with respect to legal immigrants inside this country, one of the known vectors—and, clearly, most legal immigrants who are here on special purpose visas to work for technology companies are here for legitimate purposes. But we know as a fact, we know in this Government as a fact that some of those individuals who come here legally on special purpose visas are collecting, are engaging in essentially espionage, and we know that.

At the latter—towards the latter part of the Bush administration, in fairness, in response to a number of reports from the GAO, CRS, I believe, and some inspectors general at various agencies, the Bush administration put in the pipeline a policy change that

would require employers who employ foreign nationals legally in the country to make certain certifications about those persons' access to controlled technology in the United States. That is a positive change. But this is an area that's important, and I would just underscore that I largely agree with this Ms. McNeill.

Mr. ROGERS. Great. Thank you. My time is expired.

Mr. Chairman, I do agree with the Ranking Member, and I hope that you will consider calling John Morton from ICE in here to help reconcile some of the differences that have been stated here about his performance.

I yield back. I hope you have a second round.

Mr. MCCAUL. We do intend to call him as a witness at a later hearing, because some of these numbers are disturbing to me. When I do see even the employer prosecutions convictions, they are not really of any significance. I don't think it is having a deterrent effect as we talk about protecting American jobs, you know, here in the United States.

So the other interesting point was, Mr. Mancuso, you mentioned 90 percent of the scientists and engineers are now in Asia. That's a pretty sad commentary on the state of education in the United States and the workforce.

I talked about the H1–B visas. You know, I have got the University of Texas with their Pickle Center. They train, educate these students at taxpayer expense, and then, when they graduate, they can't stay. They go back to our competitor. I just find that to be—we need a high-skilled workforce in this country, and I think that that would be a way to maybe change some of those numbers that you talked about.

So the Ranking Member and have I agreed that we are probably going to go ahead and conclude, unless the other two have questions.

But I want to thank the witnesses for their testimony. It has been very enlightening. I have a couple of action items to follow up on, particularly on the semiconductor chips. I just want to thank y'all for calling this to our attention.

Members have 10 days to submit written questions. If they do so, I would ask that you respond to those. Again, thank you for your valuable insight to this committee.

The committee stands adjourned.

[Whereupon, at 11:32 a.m., the subcommittee was adjourned.]

○