

# OVERSIGHT OF INTELLECTUAL PROPERTY LAW ENFORCEMENT EFFORTS

---

## HEARING BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

---

JUNE 22, 2011

---

**Serial No. J-112-28**

---

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PUBLISHING OFFICE

92-565 PDF

WASHINGTON : 2015

---

For sale by the Superintendent of Documents, U.S. Government Publishing Office  
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin	CHUCK GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
CHUCK SCHUMER, New York	JON KYL, Arizona
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TOM COBURN, Oklahoma
RICHARD BLUMENTHAL, Connecticut	

BRUCE A. COHEN, *Chief Counsel and Staff Director*

KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

# CONTENTS

## STATEMENTS OF COMMITTEE MEMBERS

	Page
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont .....	1
prepared statement .....	40
Grassley, Hon. Chuck, a U.S. Senator from the State of Iowa .....	3

## WITNESSES

Witness List .....	39
Espinel, Victoria A., Intellectual Property Enforcement Coordinator, Office of Management and Budget, Washington, DC .....	4
prepared statement .....	42
Weinstein, Jason M., Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, Washington, DC .....	7
prepared statement .....	50
Snow, Gordon M., Assistant Director, Cyber Division, Federal Bureau of Investigation, Washington, DC .....	9
prepared statement .....	67
Gina, Allen, Assistant Commissioner, Office of International Trade, U.S. Cus- toms and Border Protection, U.S. Department of Homeland Security, Wash- ington, DC .....	11
prepared statement .....	76
Barnett, Erik, Assistant Deputy Director, U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security, Washington, DC .....	12
prepared statement .....	89

## QUESTIONS

Questions submitted by Senator Coburn for Victoria Espinel and all wit- nesses .....	109
Questions submitted by Senator Coburn for Jason Weinstein and all wit- nesses .....	111
Questions submitted by Senator Coburn for Gordon Snow and all witnesses ...	113
Questions submitted by Senator Coburn for Allen Gina and all witnesses .....	115
Questions submitted by Senator Coburn for Erik Barnett and all witnesses ....	117
Questions submitted by Senator Franken for Victoria Espinel .....	119
Questions submitted by Senator Franken for Jason Weinstein .....	120
Questions submitted by Senator Franken for Erik Barnett .....	121
Questions submitted by Senator Grassley for Allen Gina .....	122
Questions submitted by Senator Grassley for Erik Barnett .....	123
Questions submitted by Senator Grassley for Victoria Espinel .....	124
Questions submitted by Senator Hatch for Jason Weinstein .....	125

## ANSWERS

Responses of Victoria A. Espinel to questions submitted by Senators Coburn, Franken, and Grassley .....	126
Responses of Gordon M. Snow to questions submitted by Senators Grassley and Coburn .....	164
Responses of Allen Gina to questions submitted by Senators Coburn and Grassley .....	181
Responses of Erik Barnett to questions submitted by Senators Coburn, Franken and Grassley .....	181

# IV

	Page
Responses of Jason M. Weinstein to questions submitted by Senators Coburn, Franken, and Hatch (Note: At the time of printing, after several attempts to obtain responses to the written questions, the Committee had not received any communication from the witness.) .....	223

## MISCELLANEOUS SUBMISSIONS FOR THE RECORD

American Federation of Musicians, American Federation of Television and Radio Artists, Directors Guild of America, International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists and Allied Crafts of the United States, Its Territories and Canada, International Brotherhood of Teamsters, Screen Actors Guild, June 20, 2011, joint letter ..	224
American Society of Composers, Authors, and Publishers (ASCAP), Paul Williams, President and Chairman of the Board, New York, New York, June 20, 2011, letter .....	225
Institute for Policy Innovation (IPI), Tome Giovanetti, President, Lewisville, Texas, June 20, 2011, letter .....	227
Kelley, Colleen M., National President, National Treasury Employees Union, (NTEU), Washington, DC, statement .....	228
Motion Picture Association of America, Inc., Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, Walt Disney Studios Motion Pictures, Warner Bros. Entertainment Inc., June 22, 2011, joint letter .....	236
Recording Industry Association of America, Inc., (RIAA), Mitch Bainwol, Chairman and CEO, Washington, DC, June 21, 2011, letter .....	239
U.S. Chamber of Commerce, Washington, DC, statement .....	240

## OVERSIGHT OF INTELLECTUAL PROPERTY LAW ENFORCEMENT EFFORTS

---

WEDNESDAY, JUNE 22, 2011

U.S. SENATE,  
COMMITTEE ON THE JUDICIARY,  
*Washington, DC.*

The Committee met, pursuant to notice, at 10:06 a.m., in Room SD-226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Kohl, Whitehouse, Klobuchar, Franken, Coons, Blumenthal, Grassley, and Coburn.

### OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Good morning. Sorry. We are trying to do about 40 things here at once, as you know. We have about five meetings going on at once, so I apologize for the delay starting, but I do appreciate the witnesses who are here to discuss the enforcement of our Nation's intellectual property laws. We spent a lot of time on this in the Committee in the last few months, and there is good reason for that. While estimates of intellectual property theft are hard to get exactly the amount, we know that it costs billions of dollars and hundreds of thousands of lost jobs. Now, I do not care what the economic climate is. That would be unacceptable. Of course, it is devastating today. It is not like 50 years ago where you get very excited about somebody who had a bank robbery where they stole a couple hundred thousand dollars. Most bank robbers get caught. We are talking about people who, with a key-stroke, might steal tens of millions of dollars or more.

Now, whether the property theft takes place on street corners or on the Internet, it poses a threat to American businesses, American public safety, and now we are finding even the American military. It is an epidemic. But thanks to the work of each of our witnesses, it is one that we are making significant strides to combat.

Today's hearing is almost a year to the day from our first oversight hearing for the Intellectual Property Enforcement Coordinator (IPEC) position, which was created by the *PRO-IP Act*. Several Members of this Committee cosponsored that bill, and one of the primary motivations behind creating this new position was to have one central presence to coordinate the work being done across the government to combat intellectual property theft. So it is fitting that the IP Enforcement Coordinator, Victoria Espinel, joins us again. She is joined by representatives from some of the key enforcement agencies with which she works—the Department of Jus-

tice, the Federal Bureau of Investigation, Customs and Border Patrol, and Immigration and Customs Enforcement.

The IPEC position has not been in place for very long, but you have worked very closely together, and I appreciate that. All of your agencies, as well as the other members of the Intellectual Property Rights Center, deserve credit for putting egos and turf aside and coordinating your investigative and prosecutorial efforts. This is so widespread that no one agency could handle it all. All of you working together, though, we might have a handle on it. And I know a lot of you have had to defer to another agency in pursuit of a high-profile investigation. I commend you that you have done that for the greater good. There was a time in our history when that would not have been done.

Now, Ms. Espinel, last year when you appeared before this Committee, you unveiled the IPEC's Joint Strategic Plan against counterfeiting and infringement. That plan outlined the general purposes behind your intellectual property enforcement strategy—growing the American economy and promoting innovation, protecting consumer trust and safety, and preserving our National security. And it appears you have taken some great steps in that area.

I would mention two areas in particular. The first is in criminal enforcement. The coordinated efforts of the Justice Department and law enforcement have resulted in a number of victories, including two cases involving more than \$100 million in counterfeit merchandise. The Justice Department and ICE ran a successful “Operation in our Sites” and took down 120 domain names of Web sites that were trafficking counterfeit goods.

The second advance is your ability to engage so many prominent members of the Internet “ecosystem”—including payment processors, Internet registrars, and ad networks—to come together to combat online infringement. This complements what we have been doing in Congress on the *PROTECT IP Act*, and it points out that the private sector can always do more to self-police than the government could ever enforce on its own. So we have to work together on that.

Intellectual property enforcement is a great example of a bipartisan area. The *PRO-IP Act*, for example, was cosponsored by 22 Senators—11 Democrats and 11 Republicans—and it passed the Senate unanimously. Last month we reported the *PROTECT IP Act* unanimously from the Committee. The House is currently considering another IP-related bill, the *America Invent's Act*. That we passed out of the Senate 95–5.

So there is a long way to go. I cannot emphasize how important this is. It is not just the thousands and thousands of jobs, the billions of dollars lost, but there are also great threats to our public safety and to our law enforcement and others. I will use an example of in the area of things that could be done, what happens in a part of the country like mine where it may be 10 below zero in January and somebody destroys the command and control of our power systems. That goes off into a different area, but it just shows how interdependent we are in these areas.

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

Senator Grassley.

**STATEMENT OF HON. CHUCK GRASSLEY, A U.S. SENATOR  
FROM THE STATE OF IOWA**

Senator GRASSLEY. I usually start out my remarks by thanking you for holding this hearing. I will go beyond that this time and say that not only by holding this hearing but several others you have had and the promotion of bipartisan legislation, in fact, almost a consensus formed that you need to be complimented for. But I think also beyond even helping our own economy, you are bringing attention to a lot of things that are seen as a global issue, and by your leadership and U.S. leadership in this area, doing much more good than what maybe you even anticipate, but without a doubt recognize a tremendous need in trying to solve it wherever we can. So thank you for that, including this hearing.

Our country is a global leader in innovating, creating, and developing new technology and products. The U.S. Chamber of Commerce estimated that over 19 million Americans are employed by intellectual property-based industries here in this country. The Chamber estimates that more than 60 percent of U.S. exports involve intellectual property and more than seven-tenths trillion of the U.S. gross domestic product is represented by intellectual property-related industries.

At the same time, the theft of intellectual property has skyrocketed out of control, even beyond what we most often talk about involving the country of China. A recent report estimated that counterfeit and piracy has resulted in 2.5 million jobs lost in the G-20 economies, and that brings additional emphasis to what I complimented you about, Mr. Chairman, of having a hearing here that has international implications.

Beyond the jobs lost in the G-20 countries, the global value of counterfeited and pirated goods exceeded \$650 billion. Protecting intellectual property rights is crucial to promoting innovation, creating new jobs, and advancing economic growth in the United States. Protecting intellectual property rights is also critical to keeping American consumers safe from unsafe and defective consumer products. No one intentionally wants to buy dangerous counterfeit pharmaceuticals, defective electrical products, malfunctioning equipment, and sub-par construction materials. Yet consumers are scammed all the time into purchasing these products.

I am pleased today that we hear from our federal law enforcement agencies about their efforts to enforce these property rights, both here in the United States and abroad, and how they are coordinating with each other and industry to stop intellectual property theft and how they are helping to protect the American economy and the safety of our public.

I am interested in hearing more about the Intellectual Property Enforcement Coordinator's recommendations, whether law enforcement needs more tools to go after these criminals and how the *PRO-IP Act* has helped combat intellectual property.

I just said how important this Committee hearing is, and you might wonder how important it is when I say I have to leave at 10:30 for flood issues on the Missouri River when I am meeting with FEMA people, but I am going to have to leave. And I also

want to make an excuse for Senator Hatch, who is tied up in the Finance Committee as Ranking Member there because he has always been very actively involved in intellectual property rights.

So I might be able to be back here at 11, Mr. Chairman, but if I do not get back to ask questions, then I will submit them for answer in writing.

Chairman LEAHY. Without objection, your questions and anybody else's questions will be included. I thank you, and I thank you for your compliment. It is nice to work on things that bring Republicans or Democrats together, and this is one of those areas, just as so many of you did on the patent bill.

Victoria Espinel serves as the Nation's first Intellectual Property Enforcement Coordinator. She was confirmed by the Senate in 2009. I remember that confirmation hearing very well. She is well qualified for this position. She previously served as the Assistant U.S. Trade Representative for Intellectual Property and Innovation. She was the chief trade negotiator for the United States on intellectual property issues. She was a professor at George Mason University School of Law. She served as an adviser to several committees in Congress, including this one. She received her undergraduate and law degrees from Georgetown—I am delighted to see somebody with a law degree from Georgetown—and a master of laws degree from the London School of Economics.

Ms. Espinel, please go ahead, and what we will do is I will introduce each one of you separately and each one of you will speak or give your statement. Your whole statement will be made part of the record, of course, and then we will open it to questions.

Ms. Espinel.

**STATEMENT OF HON. VICTORIA A. ESPINEL, INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, OFFICE OF MANAGEMENT AND BUDGET, WASHINGTON, DC**

Ms. ESPINEL. Thank you. Chairman Leahy, Ranking Member Grassley, Members of the Judiciary Committee, thank you for your continued leadership on this important issue.

One year ago today we sent you our Joint Strategic Plan on Intellectual Property Enforcement. Today we will be submitting to you a report on the progress made in the year since the strategy was issued. While we have taken great steps forward over this past year, much work lies ahead, and we need a continuing, coordinated response to these problems.

First let me say that law enforcement is doing great work. I feel lucky and proud to be sitting here today with these people and not just at the hearing today but every day that I work with them and their colleagues. Law enforcement agencies all have a number of priorities, but they have shown real commitment to intellectual property enforcement.

Looking at fiscal year 2009 compared to fiscal year 2010, DHS investigations and seizures of goods crossing our borders have each increased by over 30 percent, and FBI investigations are up by more than 44 percent. DOJ has bolstered State and local law enforcement by providing \$6.5 million in grants. That \$6.5 million has been used to seize close to \$200 million worth of infringing goods.



Through Operation in our Sites, DOJ and ICE have seized 125 domain names used for counterfeiting and piracy. DOJ and the FBI have increased investigation and prosecution of trade secret cases to protect against the transfer of American innovation and technology overseas. Some cases involve the theft of technology owned by our automobile industry or extremely valuable proprietary code.

Internationally, ICE now has a full-time IP-dedicated attache in China, and the FBI is preparing to do the same. The President has called for the placement of six DOJ attaches specializing in intellectual property in strategic global locations to strengthen international enforcement.

We are pressing our foreign counterparts to do more, and we are seeing greater cooperation from some governments. In June, DOJ and ICE worked with Dutch law enforcement to seize a server that was being used for piracy. ICE, working with the World Customs Organization, Interpol, and others, has targeted online sales of counterfeit medicines in coordination with 45 countries, resulting in worldwide arrests and seizures of thousands of potentially harmful drugs.

China is clearly a priority. In January, President Obama and President Hu Jintao issued a joint statement, agreeing that China will strengthen its efforts to protect intellectual property rights. China has launched a Special Campaign Against Piracy and Counterfeiting under the direction of its State Council. We are working with USTR, PTO, law enforcement, and others to assess the impact of this campaign and to press China to do more.

In addition to increased law enforcement against online infringement, we need cooperation and action from the private sector. Given the scope of the problem, we will never address it as effectively if we do not have more engagement and action from all of those who have a stake in Internet commerce.

Over the past year we have been encouraging cooperative voluntary practices to reduce infringement online that are practical and effective and consistent with important policy principles, including privacy and due process. We strongly support these voluntary agreements to help address counterfeiting and piracy online. They are complementary to increased enforcement, updated legislation, and coordinated educational campaigns.

Many rogue Web sites earn revenue through the use of online payment processing services. The major credit card companies and payment processors have now agreed to a set of voluntary best practices that provide for rapid investigation and for payment processors to withdraw their services from sites that are operating unlawfully. Starving illegal online businesses of revenue will necessarily disrupt and likely cripple the business model of many illegal enterprises. Many rogue Web sites also earn revenue through advertising, including from some of America's best-known companies. The ads for iconic and trusted brands lend legitimacy to illicit sites and can mislead consumers into believing that the sites are legitimate.

We have been working with many of the major ad networks to reach agreement on a set of voluntary best practices. While still under discussion, these best practices would limit ads being placed on sites engaged in counterfeiting or piracy. We believe that legiti-

mate companies do not want to be supporting illegal activity. We are working with a number of major advertisers and their trade associations to develop a voluntary pledge demanding that their ads not be placed on pirate sites. That process is also underway.

My office is focused on good government, saving taxpayer dollars and making sure that we avoid duplication and waste. We now have 30 law enforcement teams across the country led by ICE and the FBI that include federal, State, and local law enforcement. To better coordinate abroad, our embassies have established senior-level working groups to improve their efforts, and in April the PTO launched a public online data base that will lead to more efficient use of resources by allowing different agencies to share materials and avoid duplicative work.

We must prevent counterfeit products from coming into the U.S. Government's supply chain. We are working intensely with NASA and DOD to have recommendations to the President in early fall.

Effective enforcement against online infringement requires strong laws that keep up with technology. In March, we made 20 recommendations for legislative changes to Congress. We have been working with Congress on proposals that address illegal streaming, economic espionage, the Trade Secrets Act, and counterfeits sold to the military. We commend Chairman Leahy, Senator Klobuchar, Senator Kohl, Senator Whitehouse, Senator Franken, Senator Coons, Senator Blumenthal, and Senator Grassley for their leadership on these important issues.

Finally, we know that there is a great deal of interest in Congress in giving our law enforcement additional tools to stop Web sites engaged in substantial criminal infringing activity. This is a priority issue for us as well, and my office has convened a process to develop the administration's position on this legislation.

I commend this Committee's leadership on IP enforcement, and I look forward to working closely with you on improving protection of American intellectual property. With a unified front, we can and will defeat the criminals preying upon U.S. businesses.

Thank you.

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

Chairman LEAHY. Thank you very much.

Incidentally, I like the idea of having, as you mentioned, the people in our embassies abroad because we have always had military liaisons, agricultural liaisons, and others. They are all important, but this is extraordinarily important.

Jason Weinstein is the Deputy Assistant Attorney General in the Criminal Division, Department of Justice. In that role he oversees the Division's efforts to combat intellectual property crime, computer crime, anti-gang and violent crime, and human smuggling. Before joining the Criminal Division, he was chief of the Violent Crime Section at the United States Attorney's Office for the District of Maryland. He served as Assistant U.S. Attorney in the Southern District of New York. He received his undergraduate degree from Princeton, his law degree from the George Washington School of Law.

Deputy Assistant Attorney General, we are delighted to have you here. And did I pronounce your last name right?

Mr. WEINSTEIN. Yes, you did, Mr. Chairman.  
 Chairman LEAHY. I always worry about that. Thank you.

**STATEMENT OF JASON M. WEINSTEIN, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC**

Mr. WEINSTEIN. Good morning, Chairman Leahy, Ranking Member Grassley, and Members of the Committee. I thank you for the opportunity to be here today.

As we all know, and as the Chairman said in his opening, criminal enforcement of intellectual property rights is critical to our economic security and to the health and safety of our citizens. Piracy, the distribution of counterfeit goods, and trade secret theft threaten American companies and American jobs. Counterfeit pharmaceuticals and other dangerous products threaten our health and safety. And when counterfeit computer hardware makes it into the military supply chain, it puts our troops, already in harm's way, in even greater danger.

Technological innovations have revolutionized the way the world does business. The increasing availability of Internet access has allowed rights holders to distribute or stream digital content to a worldwide market almost instantaneously. And with improvements in manufacturing and transportation and shipping, even small businesses have unprecedented opportunities to market and distribute their goods and services around the world.

Yet as our world has become smaller, the threat posed by IP crime has grown bigger. IP criminals have exploited these same innovations to engage in every type of IP offense imaginable, from online piracy, the sales of counterfeit goods and pharmaceuticals, to economic espionage. And these IP criminals can now operate anonymously in cyberspace, committing their crimes from around the corner or around the globe.

In recognition of this growing threat, Attorney General Holder has made IP enforcement a top priority, and from the highest levels, the Department of Justice is fully committed to aggressive, effective criminal enforcement efforts, both here and abroad, to protect our Nation's IP stakeholders and the American public.

Under the leadership of the Task Force on Intellectual Property, which was formed by the Attorney General in February 2010, the Department has pursued a comprehensive strategy that includes the following:

No. 1, aggressive investigations and prosecutions of IP crime, with a particular emphasis on cases involving health and safety, trade secret theft and economic espionage, links to organized criminal enterprises, and large-scale commercial counterfeiting and piracy, particularly when it occurs online.

No. 2, training for State, local, and federal law enforcement.

No. 3, a grant program that, as Victoria mentioned, has provided approximately \$6.5 million to date to support IP enforcement efforts at the State and local level.

No. 4, extensive outreach to victims of IP crime.

And, No. 5, last but not least, close collaboration with other Federal Government agencies and with the Intellectual Property Enforcement Coordinator, who has provided outstanding leadership in

charting and pursuing the administration's comprehensive approach to IP protection and enforcement.

In all of that important work, our outstanding prosecutors at DOJ, both from the Criminal Division's Computer Crime and IP Section and from the Computer Hacking and Intellectual Property, or CHIP, Network in the U.S. Attorney's Offices, enjoy very strong relationships with our agency partners and in particular with the agencies represented on the panel with me today—the FBI, ICE, Homeland Security Investigations, and CBP—and with the national IP Rights Coordination Center.

Those strong relationships and the dedication and skill of our prosecutors and agents have led to a number of major enforcement successes, including the examples referred to in my written statement, and those cases, and many others like them, illustrate the scope of our efforts to pursue IP criminals. But they also reveal the global reach that IP criminals can have. The individuals and organizations responsible for these crimes often operate from foreign jurisdictions, and it is often impossible to identify, arrest, and prosecute them or to obtain critical evidence against them without the assistance of foreign law enforcement.

For that reason, Mr. Chairman, our work does not stop at our shores. Due to the increasingly international nature of IP crime, close coordination and cooperation with our foreign partners is critical to our success. We have also placed great emphasis on strengthening the enforcement capacity of nations overseas, from Europe to Asia, to Africa, to South America, to Mexico, both to reduce safe havens for IP criminals and to improve our ability to hold those criminals accountable throughout the world.

In pursuing this critical mission, we are fortunate to have the support of Congress and in particular of this Committee. I am pleased to have the opportunity today to discuss how our law enforcement strategy has been significantly enhanced by the additional tools and resources provided in the PRO-IP Act of 2008. We thank the Committee for its support of that Act and for its continuing efforts to identify ways to further enhance our ability to enforce IP rights and protect American consumers and businesses.

I thank you for the opportunity to be here today, and I would be pleased to answer your questions.

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

Chairman LEAHY. Thank you very much.

Our next witness, Gordon Snow, is Assistant Director for the Cyber Division at the FBI. His lengthy career with the Bureau began as a special agent in 1992. He also served in the U.S. Marine Corps for more than 10 years. Among his many roles with the Bureau, Mr. Snow has served as on-scene commander for the Counterterrorism Division in Afghanistan. He served as Director of the National Cyber Investigative Joint Task Force, received his undergraduate degree from the University of Michigan, Ann Arbor; also received an MBA from Virginia Tech and a law degree from Catholic University.

Mr. Snow, we are delighted to have you here. Please go ahead.

**STATEMENT OF GORDON M. SNOW, ASSISTANT DIRECTOR,  
CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION,  
WASHINGTON, DC**

Mr. SNOW. Thank you. I am pleased to appear before you today to discuss the Prioritizing Resources and Organization for Intellectual Property Act of 2008 and the FBI's efforts, activities, and successes relating to intellectual property rights crimes.

The enforcement of U.S. laws protecting IPR is critical to the U.S. economy, our National security, and the health and safety of American citizens.

IPR violations, which include theft of trade secrets, digital piracy, and the trafficking of counterfeit goods, result in billions of dollars in lost profits annually.

Some IPR violations pose a more far-reaching and serious threat to the U.S. than just economic loss to the rights holder. Such violations put public safety at risk through the sale of counterfeit pharmaceuticals, electrical components, aircraft and automobile parts, and the funding of organized crime. My remarks today will focus on the role the FBI plays in protecting IPR, our efforts to coordinate with other federal agencies to ensure that intellectual property is protected, and our successes in this arena.

The FBI's strategic objective is to detect and disrupt state-sponsored groups and international and domestic criminal organizations that manufacture counterfeit goods and distribute or otherwise profit from the theft of intellectual property.

The FBI partners closely with the National Intellectual Property Rights Coordination Center, which is hosted by U.S. Immigration and Customs Enforcement. The IPR Center serves as a centralized, multiagency entity for the U.S. Government's criminal enforcement of intellectual property laws, hosting weekly deconfliction meetings to ensure resources are effectively and efficiently devoted to investigations.

The FBI moved its Intellectual Property Rights Unit to the IPR Center in April of 2010. The IPR Unit provides national program management for the FBI IPR program and initiates and conducts IPR investigations that are complex, multijurisdictional, and/or international in nature.

As a result of the PRO-IP Act, the FBI has 51 dedicated IPR special agents placed in 21 field offices and the IPR Unit. Of these 51 positions, 44 special agents were placed in 20 field offices where United States Attorneys' Offices had Computer Hacking and Intellectual Property Rights Units. The locations for the distribution of these resources were selected based on a regional domain analysis of the threat to intellectual property, intellectual property threat intelligence reporting, input from the IPR Center, and an understanding that the geographically dispersed nature of IPR violations and subject locations made it possible to establish venues regionally. The placement of the special agents was coordinated with and approved by the Office of the Deputy Attorney General and the Executive Office of the United States Attorneys.

In an effort to improve international relationships on IPR investigations, the IPR Unit embedded a dedicated IPR team comprised of an analyst and an agent in the FBI's Legal Attache offices in Beijing and New Delhi to work directly with local and regional au-

thorities on IPR matters for 60 days. Based upon the results of this effort and the threat emanating from these regions, the IPR Unit is currently in the process of embedding a full-time IPR dedicated agent in Beijing for one year.

The FBI places a heavy emphasis on meaningful training and capacity building. The FBI provides IPR training to domestic and international law enforcement officials and is collaborating with its partner agencies to develop a more comprehensive and advanced intellectual property training curriculum to ensure a uniform foundation across law enforcement agencies conducting IPR investigations. The FBI also provides State and local law enforcement and industry liaisons with information about how to most effectively partner with the Federal Government in IPR cases. In fiscal year 2009, the FBI provided IPR training to 782 individuals from the Federal Government, the domestic private sector, foreign governments, and the overseas private sector. In fiscal year 2010, that number was 1,678 additional individuals within the same groups. At the end of last month, the FBI had already trained up to 1,064 individuals.

Over the past two years, the FBI provided training in IPR to law enforcement officials from 15 different countries. The FBI's use of PRO-IP Act resources has permitted an increased focus on training in high-priority areas.

Over the past year, the FBI and its partners have successfully investigated major IPR violations that resulted in millions of dollars in losses and unquantifiable harm to human health and safety. Those examples are in my statement.

The PRO-IP Act has enabled the FBI to dedicate increased numbers of special agents and analysts to IPR matters, ensure quality training, and support effective interagency collaboration. We look forward to working with the Committee and Congress as a whole to continue on a successful course forward for the Nation that protects intellectual property and its citizens.

Thank you for the opportunity to be here, and I would be happy to answer any questions you may have.

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

Senator WHITEHOUSE [presiding]. Thank you, Mr. Snow.

Our next witness is Allen Gina. He is Assistant Commissioner at the Office of International Trade for the United States Customs and Border Protection agency, a position he has held since March. Mr. Gina began his career as a customs inspector in 1983. Prior to serving in the Office of International Trade, he served as Assistant Commissioner at the Office of International Affairs. From February 2003 to May 2004, he was detailed to the Directorate of Border and Transportation Security to help set up the Department of Homeland Security. He received his undergraduate degree from Queens College in New York, is a graduate of the Kennedy School of Government Senior Executive Fellows Program, and we welcome him today.

Mr. Gina.

**STATEMENT OF ALLEN GINA, ASSISTANT COMMISSIONER, OFFICE OF INTERNATIONAL TRADE, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC**

Mr. GINA. Good morning, distinguished Members. Thank you for the opportunity to discuss the actions we are taking at Customs and Border Protection to ensure that the laws governing intellectual property rights are properly enforced.

Having spent the past 29 years of my career with CBP and previously the U.S. Customs Service and having been a uniformed inspector, I have firsthand experience of the challenges CBP encounters daily to protect our National security while also facilitating the flow of legitimate trade and travel and enforcing trade laws.

As you know, CBP targets goods entering the United States, and we detain and seize merchandise that infringes trademarks, trade names, and copyrights. We also assess fines and penalties against violators and enforce exclusion orders issued by the International Trade Commission. Our office's import specialists, trade specialists, auditors, lawyers, and other disciplines are trained in the many facets of international trade to take into account the ever-changing challenges at over 300 ports of entry.

In addition to our own staff, CBP partners with other federal agencies, foreign governments, and the private sector. Our closest partner in IP enforcement is, of course, our sister agency, ICE, which is the investigative arm of DHS. Within the U.S. Government, we also work closely with Ms. Espinel's office to ensure a coordinated U.S. Government response to IP theft as envisioned in the PRO-IP Act.

Internationally, we actively engage our trading partners to share best practices, exchange information, and conduct joint enforcement operations. For example, we are conducting a joint enforcement operation focusing on counterfeit pharmaceuticals shipped via international mail and express consignment with 11 members of APEC. In addition to our collaboration in APEC, CBP strengthened its engagement with China customs by amending the Memorandum of Cooperation on IP Enforcement that our two agencies signed in 2008. Last month, I signed letters of exchange with my counterpart from China customs to remove all limits on the amount of information that we can share.

When goods arrive at our borders, CBP inspects targeted shipments and seizes, forfeits, and disposes of the counterfeit and pirated goods. Last year alone, cooperative efforts by CBP and ICE resulted in 19,959 seizures. This year we are on pace to reach 25,000 seizures. This is in comparison to 3,500 seizures made in 2001 and 14,600 seizures made in 2006.

Our seizures also lead to criminal convictions such as the federal conviction of an individual who trafficked in counterfeit Cisco equipment that Mr. Barnett will be referring to.

Nevertheless, CBP recognizes that we must continue to improve our enforcement efforts. The appropriation from Congress will help us do so. We plan on spending the funds on human capital, technology procurement, training, and travel for outreach and temporary duty assignments to support IPR enforcement.

CBP identified several challenges in its five-year strategy on IPR enforcement which was delivered to Congress in 2010, including a need for additional advance information, the high quality of counterfeit and pirated goods which is making infringement determinations more challenging, and the need to enhance our partnerships with the trade community. We are working to resolve these issues, and we have a number of initiatives to guide us that are included in the IPEC's Joint Strategic Plan and our own five-year IPR strategy.

To improve the information available for targeting, we initiated the pharmaceutical Center for Excellence and Expertise pilot in November. The center works with industry stakeholders to enhance CBP's understanding of and centralize our knowledge of private sector business practices. Last month, the CEE personnel conducted an enforcement operation in which they worked with ICE and DOJ to obtain three criminal warrants.

To combat the improving quality of counterfeit and pirated goods which makes infringement determinations increasingly difficult, we are working with the IPEC to identify legislative recommendations that would allow CBP to share information with right holders to leverage their expertise. With your assistance implementing these recommendations, we will be able to take dramatic steps toward enforcing IPR at the border.

I thank you again for the opportunity to appear before you today, and I would be happy to answer any of your questions. Thank you.

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

Chairman LEAHY [presiding]. Thank you very much.

Our next witness is Erik Barnett. He serves as Assistant Deputy Director for Immigration and Customs Enforcement, which we know as ICE. His responsibilities in this position include intellectual property theft enforcement, narcotics trafficking, human rights violations, and war crimes, among others. That is a pretty big portfolio.

Mr. BARNETT. Yes, sir.

Chairman LEAHY. Prior to joining ICE, he served as Assistant U.S. Attorney in the Eastern District of Virginia, where he was chief of the Narcotics and Dangerous Drug Unit. He spent some time on this Committee, as we all know, as the legislative fellow for Senator Durbin. He received his undergraduate degree from the University of Arizona, law degree from California Western School of Law.

Please go ahead, sir.

**STATEMENT OF ERIK BARNETT, ASSISTANT DEPUTY DIRECTOR, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC**

Mr. BARNETT. Good morning, Mr. Chairman, and I thank you and Members of the Committee for the opportunity to discuss ICE's efforts in intellectual property theft enforcement.

With the Committee's indulgence, I will begin my remarks just by walking you through one of ICE's very recent successes in IP theft enforcement.



Less than two months ago, the Fifth Circuit Court of Appeals affirmed a criminal conviction for trafficking in counterfeit Cisco network cards. The defendant had a contract to sell genuine Cisco network cards to the United States Marine Corps. The court noted that the criminal case began when a shipment from China was intercepted by a CBP officer who suspected that the Cisco parts were not genuine and were counterfeit. CBP informed an ICE agent, who contacted and interviewed the defendant. The case involved ICE, the Defense Criminal Investigative Service, and the Houston United States Attorney's Office and resulted in the defendant being sentenced to 51 months in a federal prison. That was the high end of the Sentencing Guidelines range.

We submit respectfully that there are three very important points that arise from this significant intellectual property theft case.

First, ICE cannot achieve success in IP theft enforcement without partnerships with other key law enforcement agencies, many of whom are represented today at this table.

Second, ICE needs the support of the private sector to thoroughly conduct criminal investigations. Cisco Systems worked diligently with our agents on identifying the counterfeits and assisting with the investigation.

Finally, and clearly the most troubling, is that counterfeiting is no longer limited to luxury brands and high-end goods. It has infiltrated almost all segments of commerce. Wherever there is a price point at which criminals can make a profit with absolute disregard for the significant impact on public safety, just in the past year, ICE has seen cases involving fake cancer drugs and heart medicines, phony circuit breakers that could have been built into homes, and counterfeit airbags destined for used cars. ICE has received a fair amount of recognition for our increased IP theft enforcement over the past two years. In particular, since last June we have engaged with the Justice Department in innovative enforcement through Operation in our Sites against Web sites that commit IP theft.

At ICE our intention has been no less than to change the face of IP theft enforcement in the United States through vigorous and consistent investigation and prosecution. But our efforts do not—cannot—occur in a vacuum. CBP, FBI, DOJ, and Victoria Espinel's office have all worked steadily with ICE over the past two years on moving forward. We have also enjoyed the assistance of State Attorneys General and local law enforcement through 26 local IP Theft Enforcement Teams, also known as IPTETs. These were developed last year by ICE at the IPR Center to attack IP theft at all levels throughout the country. We work with DOJ to provide training for each of the IPTETs.

Our successes have been achieved through the dedicated efforts of our agents, more than 7,000 of whom are in ICE's Homeland Security Investigations, whose mission to combat IP crime comes from one of our legacy agencies, the U.S. Customs Service. Mostly, though, our success has been made possible through the joint efforts of agencies at the National Intellectual Property Rights Coordination Center, also known as the IPR Center, that although led by ICE, consists now of 19 partner agencies, including FBI and

CBP. The existence of the IPR Center is a recognition that no one law enforcement agency alone can take on IPR theft enforcement.

That recognition sparked the announcement last week of Operation Chain Reaction, a specialized enforcement action involving ICE, CBP, FBI, DOJ, and the relevant military investigative agencies, as well as the General Services Administration, at the IPR Center. Operation Chain Reaction will specifically target for investigation individuals that attempt to sell counterfeit goods to the military and other U.S. Government agencies.

Thank you again for the opportunity to testify, and I would be pleased to answer any questions.

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

Chairman LEAHY. Well, thank you very much.

You know, you talked about the artificial airbags, for example, or counterfeit airbags. We have also seen it with brake pads and everything else. And sometimes people think that with these counterfeit goods it is like buying a handbag or a belt holding a brand name from a street corner. That is one thing, and that is wrong, too. But these are things that you can end up dying as a result of it.

In counterfeit drugs, we have seen that with cancer patients and others, the high cost of drugs. Well, you can buy it somewhat less on one of these things, but it is useless to protect their lives. Those things worry me, as I know it does you.

Ms. Espinel, I was glad to see what you have done to bring the private sector together on intellectual property and infringement. You had several members of the Internet ecosystem, payment processors, advertisers, networks, registrars. They formed a nonprofit to combat illegal pharmacies, which goes to what I was just saying here. Those go well.

How extensive do you think this voluntary action can be? Is this a real tool that we can count on in the future?

Ms. ESPINEL. I think it could be enormously important, and that is why my office, with the Administration as a whole, including the President and the Vice President, have been so supportive of this approach. You have sites that are selling illegal goods and services, and if pay processors are not engaging with those sites and are not processing those sorts of illegal transactions, they no longer have a financial incentive to sell.

You have sites that are supported by advertising, which is problematic both in that it is giving those sites a source of revenue but also, as I mentioned, it is making sites appear legitimate when they are not. If we can get both the ad networks that place those ads and the major advertisers online to step up and take steps to make sure that ads are not placed on those sites, I think that could be enormously important, again, both in terms of cutting off the revenue source and in making those sites seem less legitimate.

Internet service providers have interaction with obviously subscribers across the United States. I think having ISPs engage in educational activities so that the customers they interact with are aware that they are engaging in what is illegal activity I think can be enormously valuable. Domain name registries and registrars—obviously the ones who essentially are leasing the names of the

Web sites—have an important role to play, and we have found them to be very cooperative in our efforts and also—I will let law enforcement speak to this, but also engaging with law enforcement.

Chairman LEAHY. You mentioned a challenge there, and the advertisers, it is an area that really bothers me, and you have put your finger on it. It is not just the revenue they get. It is the verisimilitude they give to the site, and that bothers me a great deal. I can think of some these advertisers that have done this, and at some point I would hope that they would realize voluntarily they should work with you because, otherwise, there will have to be real pressure from the Congress on this.

Let me ask each one of the rest of you. We can talk about successes, and there have been a lot. What would you say—we are the legislators, we are the appropriators. We have to have some idea of where we are going. What would you describe as the greatest challenge that your agency or your office faces related to intellectual property enforcement? If you could do it briefly, what is the greatest challenge? Mr. Weinstein, I will start with you first.

Mr. WEINSTEIN. Mr. Chairman, I think it is the international/transnational nature of IP crime, and particularly as it relates to online piracy. You know, as I said in my opening remarks, the fact that the crime could be committed by somebody sitting in an apartment somewhere in a country in Eastern Europe just as easily as if the person was in this building makes it a particular challenge. And as you know, there are a number of particularly difficult things that make international cases challenging generally and they make online cases challenging in particular: the need to collect electronic evidence, the need to follow the trail of proxies and other anonymizing technologies used by these criminals to try to protect their identity when they are committing the crime, and the fact that they are often in countries where they believe that they have safe havens. And so for that reason, one of the things we try to do is work with our foreign partners to reduce safe havens overseas.

Chairman LEAHY. It is not like a bank robbery where you could look at the surveillance cameras.

Mr. WEINSTEIN. That is right.

Chairman LEAHY. Mr. Snow.

Mr. SNOW. Senator, I would echo what Mr. Weinstein just said, the international nature of not only the cyber threat itself, but the global proliferation on the Internet and how it brings into this a harder investigative road to go forward. I would add to it also just an extreme knowledge and insight that we can bring to the private sector in that partnership. I think there have been years where the private sector has thought that we would want to push off, from the law enforcement side, investigations, number one; or, two, that we did not have the time to look at those investigations and address them as seriously as we have in the last two years.

Chairman LEAHY. That is encouraging.

Mr. Gina.

Mr. GINA. Sir, CBP being a non-investigatory agency but one that interdicts, you know, apprehends, and seizes, I think a significant challenge for us is actually determining the legitimacy of goods and/or based on current technology the quality of counterfeits

has so significantly improved, being able to partner with the appropriate right holders to make those determinations is probably one of the most significant challenges for CBP.

Chairman LEAHY. Interesting. Thank you.

Mr. Barnett.

Mr. BARNETT. Mr. Chairman, one of the benefits of being last is I can certainly agree with everything that has just been said, and I do.

The other thing I would mention is that a disturbing trend in terms of enforcement capacity is that ICE and CBP seizures in fiscal year 2010 of parcels coming into the country that are valued—manufacturer's suggested retail price of counterfeiting that is valued under \$1,000, seizures increase 40 percent. More and more counterfeits are coming in through the parcel services, so FedEx, U.S. Mail service, otherwise. And while we are still seeing the 14-foot cargo containers that allows you to seize hundreds of thousands of dollars worth of counterfeit goods at a time, there are some real resource challenges but also investigative challenges in terms of working backwards from a parcel.

So a lot of this I think is—as Mr. Weinstein said, a lot of this is because this has become Internet-based shopping, and the pharmaceuticals are still coming in that way as well.

Chairman LEAHY. I was going to say, a pharmaceutical is an easy one to send that way.

Mr. BARNETT. Yes, sir.

Chairman LEAHY. Well, I appreciate this. Before I yield to Senator Coburn, who has been waiting here patiently, I just wanted to ask consent to insert in the record letters and statements from various outside groups: the U.S. CMS, Recording Industry Association of America, the American Federation of Musicians, and others, American Society of Composers, National Treasury Employees Union, Institute for Policy Innovation, Motion Picture Association of America, a number of studios and a number of others.

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

Chairman LEAHY. I thank you very much.

Senator Coburn.

Senator COBURN. Mr. Chairman, first of all, let me thank you for having this hearing. I think it is tremendously important. We lose hundreds of billions of dollars of GDP to intellectual property theft every year, and I want to thank each one of you personally for what you do. I think the idea that we are now starting to see coordination through the various agencies is very helpful and I think is sending the signal.

Let me start my questions with Ms. Espinel and let me thank you again for what you are doing. You said that it is underway to see the ads not going on these rogue websites. Do you have any idea when you are going to be able to accomplish that?

Ms. ESPINEL. That is an excellent question. We are pressing very aggressively on it. Obviously, it ultimately lies in the hands of the private sector, so our role as government here is really to encourage and convene and facilitate a discussion and to let them know how important this is for the administration.

I would hope that we could see sort of a final agreement here within the next few months. I think we have made some progress, and I think we have a lot of good will that we are working with. So I would hope that within the next few months we would be able to say that we had agreement. But I will also say that hearings like this one and other ways that Congress can demonstrate, including I know how important this issue is for you, I think that is enormously helpful to our efforts not just on the voluntary cooperation but in general. And if this is something that is important to Congress, that is useful for us to know. I think that it is also useful for the community at large to know.

Senator COBURN. Today it is not a violation of any law that you intentionally know you are going on a rogue Web site to place an ad there. There is no violation of federal law, is there?

Ms. ESPINEL. I will take advantage of having the expertise of DOJ on this panel to defer questions, but I will say that I think, you know, there are definitely areas involving Internet stakeholders and online infringement where the law is murky, and that is one of the reasons that we think, you know, regardless of the status of the law, companies need to step up and do more.

We think the first best approach would be to have the private sector driving that effort and enthusiastic about it rather than moving to more, say, heavy-handed—but I would also want to say that ultimately our goal is to drive down online infringement, and so if the approach that we are very enthusiastic about and think it is going well, if that ultimately turns out not to be successful, then, of course, we will reassess.

Senator COBURN. Okay. Mr. Weinstein, I noticed that under the appropriations under the PRO-IP Act you did not receive the funding for the grant authorization, but the appropriators gave you other funding that you were allowed to use. One of the things that concerned me about what I saw on this is we are using nonprofits to train rather than government staff. Why is that? Do we not have capable staff which we can train rather than—and we limit the grants, but we do not limit the grants to nonprofits. We limit the grants to the States. Could you just clear that up for me?

Mr. WEINSTEIN. I would be happy to, Senator.

First of all, the appropriations we got, where there were actual monies provided, were the monies that we used to hire the new prosecutors, the new agents. The grant program, as you indicated, was not funded, but our Office of Justice Programs used discretionary funds, about \$6.5 million and counting, to provide those grants.

The three nonprofits that were among the 27 grantees who received some of that money received the money because one of the things that they can do a little more easily than we can do with government contracting rules is actually set up the trainings. The substance of the training was provided by government experts, so our folks did participate in the trainings and were the experts in the room who were doing the instructing. But some of the nonprofit grantees just can contract for space and handle the logistics of arranging a training session a little more easily than we can.

Senator COBURN. Okay. I am about to run out of time. Mr. Gina, you talked about your increase in seizures on counterfeit goods and

the ability—you do have the ability to assess penalties in the form of monetary fines. Between 2001 and 2006, you assessed \$1.1 billion in fines. You only collected \$2.7 million. You noted that since 2006 the increased assessment of penalties and collection of penalties, but the collection only went up by three percent. Why is it that we have so much trouble collecting the fines that you assess?

Mr. GINA. Our attempt is to reach the individuals who are ultimately accountable, and we have been challenged in having those individuals pay the penalties. At the direction of Commissioner Bersin, he has asked us to look at our penalties and our mitigation process to actually see if we can go against other individuals that may have a financial connection or a nexus to those individuals. Very similar to areas such as antidumping, countervailing duty, we have foreign-based importers of record who, when we go to assess the penalty, they are outside the reach of CBP, but the Commissioner has asked us to review that.

Senator COBURN. All right. Thank you.

Mr. Chairman, I will have the rest of my questions for the record.

Chairman LEAHY. Thank you, and I appreciate the questions you had here.

[The questions of Senator Coburn appear under Questions.]

Chairman LEAHY. Senator Kohl.

Senator KOHL. Thank you very much, Mr. Chairman.

Ms. Espinel, your office issued a report earlier this year that called economic espionage one of the most serious intellectual property crimes facing our country. Nearly 80 percent of Fortune 500 companies' market value is in intellectual property, including trade secrets, and they lose billions of dollars when criminals steal them.

As you know, I have introduced legislation to increase penalties for economic espionage, and we have been working with your office on it. This bill is a small but important step in updating and modernizing the 1996 law that made economic espionage a federal crime. Can we count on your support for our legislation?

Ms. ESPINEL. Absolutely. We think this is an enormously important issue. Trade secret theft in general, because of the negative impact that it has in taking the technology and innovation that is developed by American companies, is one of the worst types of IP crimes, and then economic espionage, where a foreign government is involved, is even more egregious. So we think it is an enormously important issue. We say it all the time, but it is absolutely true that our intellectual property is our global comparative advantage, and if we are losing it to other countries, it has enormous repercussions for our economy, and we look forward to working very closely with you on the legislation that you introduced, and thank you for your leadership.

Senator KOHL. Thank you so much. We have heard, Ms. Espinel, from companies and lawyers who advise them on trade secrets that they would be aided in their fight against economic espionage if they could bring private lawsuits in federal court. Would you support creating a federal private right of action for trade secret theft?

Ms. ESPINEL. It is something that we would seriously consider. We have had some preliminary conversations with the Department of Justice about this, and I can commit to get an answer to you on

that issue. I know it is something that you are interested in. It is not something that we have a final position on, but I can tell you, as a general matter, as I said, this is a very important issue to us, and if a private right of action would be beneficial to our law enforcement, then I think it is something that we would at least seriously consider, if not support.

Senator KOHL. Would it help, Ms. Espinel, trade secret owners better protect their businesses if they had this right?

Ms. ESPINEL. Since there is no formal administration position on this, I would prefer not to give a formal answer at this time, but I can promise you that we will consider it. As I said, we have already had some preliminary discussions with the Department of Justice. We will turn up the volume on those discussions and be back to you as soon as possible.

Senator KOHL. Okay. Thank you.

Mr. Weinstein, do you support my legislation to increase criminal penalties? Do you think there are any additional changes that need to be made to the Economic Espionage Act of 1996 to improve its effectiveness?

Mr. WEINSTEIN. Senator, we do support your bill. We think it is a good idea, and I think its intent is consistent with the proposals that are in the white paper that Victoria's office sent to Congress in March. And we appreciate your leadership on this issue as well.

We have been working with your staff, as I think you know, to provide technical assistance and are happy to continue to do that.

There is not anything that comes to mind that I think could make the bill stronger. I know that there is frequently discussion about whether legislative changes are needed to give us additional tools to protect trade secrets during the course of investigations and prosecutions, that is, to give companies greater comfort that their secrets will be protected during the course of a criminal case. And in our view, although we are always happy to explore other options, it is our view that that is not so much an issue of whether we have adequate tools, but whether companies are sufficiently educated about the tools we do have.

Section 1835 gives courts very broad authority to fashion orders and appropriate remedies to protect trade secrets during criminal cases, everything from—you know, the statute gives the court authority to do whatever it wants, but the tools include, you know, closing a courtroom, making orders that provide that the trade secrets are available only for the attorney's eyes, protective orders, things of that nature. And what we have been trying to do, both the FBI and DOJ, has been to educate victim companies at conferences and other meetings we have with victim companies throughout the country about those tools, to give them greater comfort that if they come forward and they assist us in investigations and prosecutions, their trade secrets will be protected. And we have got a number of examples from major companies—Goldman Sachs, Societe Generale, whose name I just butchered, Ford, Dupont, Dow Chemical—major U.S. companies that have come forward and, I think been responsive to the training and education we have been doing with them and that they have more comfort and confidence that their trade secrets will remain protected while we try to vindicate their rights in a criminal court.

Senator KOHL. Thank you. Quickly, a last question. For many years, the Department of Justice was slow to prosecute economic espionage. Recently, DOJ has stepped up enforcement and has had a number of successful high-profile convictions, yet we have heard from stakeholders that they are hesitant to report economic espionage to Justice because they are concerned that it will not prosecute cases unless they are high-profile, slam-dunk cases and that their trade secrets may not be fully protected during a trial.

What can we do to address these concerns?

Mr. WEINSTEIN. Well, taking the second one first, I think as I said we need to do more. We have been doing quite a bit, both the FBI and Justice, to try to educate potential victims that their trade secrets will be protected and that we have got the tools to do that. But obviously we need to be constantly vigilant and make sure that we are doing even more to make sure that victims have that comfort.

With respect to the first characterization, I just respectfully disagree with anyone who would say that. The fact is trade secret cases are inherently difficult. They are time-consuming. Some are more difficult than others, but Justice does not shy away and the FBI or the law enforcement partners do not shy away from difficult cases. In fact, I think we are drawn to them. If people feel that trade secret cases are taking a long time, it is not a reflection of our lack of desire or focus on them. It is a function of the complexity of the case.

I can tell you that the IP task force that I mentioned in my opening remarks that the AG created last February has made the prosecution of trade secret and economic espionage cases one of the highest priorities for him personally and for the Department. So throughout the country, not just at CCIPs but in the U.S. Attorney's Offices and the FBI, we are seeking those cases out, and we are aggressively pursuing them.

Senator KOHL. Thank you, Mr. Weinstein.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Senator FRANKEN.

Senator FRANKEN. Thank you, Mr. Chairman, for this important hearing, and thank you all for the work that you are doing.

I have a question that is really for anyone who wants to answer it. It is about China. I am probably the only Member of the Committee who made most of his living creating intellectual property, so I have a special interest in this hearing.

Mr. Weinstein, I know you mentioned China as an emphasis and also online activity as an emphasis. What percentage of the Chinese people are online?

Mr. WEINSTEIN. I do not know the answer to that question, Senator. I do not know if Victoria does.

Ms. ESPINEL. I do not know the answer to that question, but I know that it is a lot. And, in fact, one of the things that we are seeing in China—

Senator FRANKEN. There are a lot of people in China.

Ms. ESPINEL [continuing]. Is sort of sites that are very similar to U.S. sites, you know, Chinese versions of eBay and Facebook and



Google being developed in China because of the number of people that are online.

Senator FRANKEN. I noted the special emphasis on China and the Internet, but the vast majority of people in China are not online. What I am interested in is enforcing that copyright infringement, too. I have seen a report that the private DVD industry—this is the physical DVDs; this is not online—in China brought in over \$6 billion in 2010. What are we doing about that?

Ms. ESPINEL. I will mention a few things, but then I may also call on my colleagues to speak as well. It is absolutely true that in China and in other countries around the world we have a huge physical problem in addition, frankly, in China, to also a growing online problem. But the scope of the physical problem in China both in terms of impacting the domestic market in China and in terms of counterfeit goods, physical goods that then get exported out of China around the world, is a big problem. I will just mention a few things.

First, China is clearly the priority focus in terms of countries overseas, and there is no other country in the world that is receiving the amount of pressure from the U.S. Government that China is, and that includes President Obama has raised this repeatedly with President Hu Jintao, but it has also been raised by senior-level officials across the administration.

The Chinese launched Special Campaign Against Counterfeiting and Piracy, and while they have launched campaigns in the past, this campaign is being led by the State Council, which is sort of like the Chinese equivalent to the Cabinet, and it is overseen by their Vice Premier. So it is a much more senior and much more coordinated campaign than any that China has launched in the past.

One of the things that we are engaged in right now is working with law enforcement agencies here that have people on the ground—industry, USTR, PTO, and others—to find out exactly what happened in that campaign. The Chinese set out 10 to 12 goals that they were going to address and see which of those they have actually made progress on, which they have in some, and where they are deficient and press them to do more in the areas where they are deficient.

Two other things that I would mention just briefly. Part of what—we need to have foreign law enforcement, including Chinese law enforcement, more engaged, and Attorney General Holder was in Beijing, in China, and he made it very, very clear to his counterpart that there needed not just to be nice high-level discussion between the Attorney General and his counterpart, but actual on-the-ground cooperation from foreign law enforcement. Attorney John Morton of ICE and Alan Bersin of CBP were also in China within the last nine months pressing their counterparts to do more.

Beyond pressure, I think we also need to have people on the ground in order to build those day-to-day relationships, which is why I think it is so important that the agencies here are all having attaches or essentially law enforcement personnel placed on the ground in China to help build those relationships directly.

The last thing that I would mention is USTR this year for the first time did a special report on what they call notorious markets. So those are both physical markets and online markets that exist.

Many, as you probably will not be surprised to hear, are in China, and the purpose of the report is to get Chinese law enforcement to do more, so to encourage countries to actually be enforcing in their own backyard.

One of the benefits of those, we have seen not just increased law enforcement, for example, from the Hong Kong authorities coming out of that report; we have also seen in the online environment some of the Chinese sites, at least one big Chinese site sort of voluntarily say that they were going to take action because they were unhappy about being on the USTR list.

With that, I have taken a lot of time, so I am going to pause, if any of my colleagues would like to add to that.

Mr. WEINSTEIN. The only thing I would say, Senator, is that there is virtually no type of IP crime for which China would not be at or near the top of the list of concern. It is not just piracy and it is not just online piracy, but it is manufacturing counterfeit DVDs, it is fraudulent software, it is counterfeit goods, trade secret, economic espionage. China is all over some of our biggest cases in that area, too.

From a law enforcement point of view, what we emphasize is bilateral engagement with Chinese law enforcement. CCIPs is part of a working group with the Ministry of Public Security to try to identify cases where we can help each other exchange evidence, cases we can work together jointly. We had one big case back in 2007 in which we took down—helped the Chinese take down a ring of 25 people who, according to Microsoft, were manufacturing \$2 billion in counterfeit Microsoft software. But that is just one case, and one case four years ago. And so what we want from China is not just encouraging signs but enduring commitment. We want the Chinese to match their words and the promises with action, and we intend to keep the pressure on to make sure they do that.

Mr. SNOW. And, sir, I will make one quick statement. Obviously, in our international outreach from the law enforcement side, and particularly in this case from the FBI, we found out in all the cyber threats that the people that we embed, not just the people that we have at the embassy, but the people who wake up every day and work on the computer crime investigative units across the world, when we embed a person from the FBI or from law enforcement there, it just moves that relationship so much further forward. It makes sure that we have the correct connectivity and much more success.

Obviously, I do not think that we will be able to embed somebody over in the Ministry of Public Security, but we do have somebody that is going to be attached directly to the embassy in Beijing. We are selecting that person now. We have a full immersion Chinese speaker that will go over there and try to make that relationship between law enforcement, you know, with the direction of the—and the guys of the Department of Justice in the Intellectual Property Coordination Office would like to go to see if we can work on those issues, and we have engaged our Director of Intelligence to evaluate those threats that are over there.

Senator FRANKEN. I am sorry I went over my time, Mr. Chairman. I want to note the USTR, as Ms. Espinel mentioned, and or China has certain trade obligations to us. I hope we enforce them,

and I hope we are working with the USTR and WTO to clamp down on this huge problem.

Thank you.

Senator WHITEHOUSE [presiding]. Chairman Leahy had to go to another hearing that is scheduled. As everybody on the Committee and everybody on the panel knows, he has been a real champion on these intellectual property enforcement issues, but he had to excuse himself for another hearing, so I will carry the gavel for him for the remainder of this hearing, and I recognize Senator Coons.

Senator COONS. Thank you, Senator Whitehouse, and thank you to everybody on the panel for your very determined hard work in this field, for your testimony in front of us today, for your obvious coordination and enthusiasm in taking on what I think is one of the most important strategic challenges facing the United States. If we are to sustain our competitiveness, if we are continue to be the world's innovation leader, and a vibrant economy, we have to get this right. It is something that I think the administration has brought a new level of focus and coordination to, and I just wanted to commend you for that.

I had a chance to meet with USTR Ron Kirk earlier this week and highlighted the importance, in my view, of additional enforcement resources, additional assertion of American rights. As Senator Franken mentioned, I think we are, frankly, losing, have been for more than a decade losing huge amounts of American intellectual property of all different types. Senator Kohl's work on trade secrets, I think, is particularly important. I am pleased to hear about your enthusiasm for pursuing that.

I wondered, Mr. Snow and Mr. Weinstein, if you might just briefly mention—we have dedicated a lot of this conversation to state actors and to private actors within states such as China, but can you just comment about links you may have seen between IP theft and organized crime or terrorist organizations, whether in the U.S. or abroad, and what DOJ in particular is doing about that.

Mr. WEINSTEIN. Sure, Senator. As you know, I think in the PRO-IP Act, one of the things the statute calls for is to have law enforcement engage in an effort to identify links between IP crime and organized crime, and we have taken that to heart.

The Attorney General has directed us to make sure that we do everything we can to make sure that our IP investigators and our organized crime investigators are sharing information. One of the things that we did was have all of the agencies that do IP investigations input all of their data into what we call IOC-2, which is the International Organized Crime Intelligence Center, to try to identify links between organized crime groups and organized crime investigations and IP crime, and those links exist and they are being pursued. I cannot obviously talk about particular investigations, but those links have been found and are being pursued.

What we are finding with IP crime, especially online piracy, is that it is increasingly being committed by nontraditional organized crime groups. These are sophisticated criminal organizations, and it is not just piracy. One of the bigger counterfeit goods cases we took down involved a group that was operating at eight manufacturing plants in China, 13 shell companies, and was, in every sense of the word, an organized crime group. But I think the statute is

really focused more on, you know, old-school organized crime, and new-school organized crime, you know, transnational organized crime groups, that is something that we have been pursuing.

We also have been cross-training the IP investigators and organized crime investigators to be able to understand the work each other is doing, and we are trying to get them to work together as much as possible in cases.

Senator COONS. Three things, if I could.

First, we just had a field hearing in Delaware on Monday where deconfliction and the importance of Fusion Centers and sharing was referenced, and I wondered if, Mr. Barnett, given some of your previous testimony and given your comment, if deconfliction of ongoing investigations was an important tool.

Second, just on the point you were just on, under Section 402(b) of the PRO-IP Act, Congress was to appropriate funds for the AG for exactly this purpose. The written testimony suggested we have not. I am new here. Should we?

And then I have a last question for Ms. Espinel.

Mr. WEINSTEIN. I guess I will take it before I turn it over to Erik to talk about deconfliction. I guess I will take the money question.

I am not in the habit of turning down money when people are offering it to me, but I think that notwithstanding the fact that that portion of the bill was not funded, it is something that we have taken on enthusiastically. Obviously, these investigations, even those that do not involve organized crime but particularly those that do, are resource intensive, and they take a lot of time, and because they are by their nature international, you know, they are more complicated and more expensive than other cases.

IOC-2 as an entity, which is critical to our ability to identify links not just between OC and IP crime, but among organized crime cases throughout the country generally, I think has not been funded at the level that perhaps it could be. But, you know, obviously we support the President's budget request, and I think that the most important part of that budget request from an IP point of view is not about organized crime, but is the position that Victoria mentioned in her opening, which is the proposal to create six international CHIPS to work overseas, which is an expansion of a program we have had in place for three or four years called the IPLEC program, IP Law Enforcement Coordination program, which are positions that we embed overseas in our embassies who work in—one for three or four years worked in Eastern Europe; the other continues to work in Asia—to train law enforcement to build capacity in the regions in which they are operating, to work on joint investigations with those foreign countries, and to help U.S. prosecutors who are investigating and building cases here in the U.S. get the evidence they need and get the targets they need when those people or that evidence is located overseas.

So we enthusiastically support that portion of the President's request, and we think it is a critical investment in our ability to fight IP crime as we move forward in this century.

Senator COONS. I can see that my time has expired, and not wanting to go over my time, I will simply say how grateful I am for the testimony of the panel and the opportunity to follow up on some of the proposals in your white paper. And I know Senator

Klobuchar, who has taken the lead on that, may well ask questions that I would have asked about misperceptions of our cosponsored bill. So thank you very much for your appearance before the Committee.

Senator WHITEHOUSE. And we can, of course, have a second round for further questions, but now it is my pleasure to recognize our distinguished Ranking Member, Senator Grassley.

Senator GRASSLEY. Thank you. I have three questions. I may not get to all of them because I want three people maybe to look at the first one, Espinel, Weinstein, and Barnett. What additional tools would you like to see enacted into law that would assist you in your efforts to protect intellectual property both here and abroad?

Ms. ESPINEL. I will speak to that briefly, especially since you wanted to hear from others on the panel, but there are three things that I would highlight.

One is we believe the ability to have increased penalties in certain areas would be helpful, and those are for the types of IP crimes that we consider to be particularly egregious, including economic espionage, IP crimes that would have a serious risk to health and safety, sales to the military. There are certain—you know, as the intellectual property infringement problem has expanded, there are certain types of crimes that are particularly reprehensible and for which we think we may need increased penalties.

The second thing I would mention is we need to make sure that our laws are keeping pace with technology. One thing I would highlight in this regard is the problem of illegal streaming from the Internet and making sure that our laws are sufficient to allow our prosecutors to bring the cases that they want to bring. And generally, in terms of getting law enforcement tools, obviously we want to make sure that they have what they need in order to do the jobs that they do every day. I believe this has already been mentioned, but I will just mention briefly one of the problems that we have that we understand law enforcement is facing at the border is a restriction on their ability to share certain types of information with rights holders, which makes it harder for them to do their job, and that is something that we think would be very useful to have fixed.

Senator GRASSLEY. Thank you.

Mr. WEINSTEIN. Senator, I will be brief. Senator Whitehouse has never heard me give a brief answer to a question before, but I will be uncharacteristically brief.

In addition to streaming, which Victoria mentioned, and the increase in penalties, which we support, there is a proposal in the white paper to grant wiretap authority for IP cases so that we can intercept wire and oral communications as well as electronic communications. Especially as we fight IP crime that is related to organized crime, that is an increasingly important tool.

Then the I-CHIPS, which is not a new legislative tool but an appropriation that we support that would help us.

Senator GRASSLEY. Okay. Mr. Barnett.

Mr. BARNETT. Thank you, Senator Grassley. I would echo what my colleagues said, and certainly with Victoria's white paper, as you well know, that was an interagency process that she, frankly,

boldly and thoughtfully undertook. So those really represent the administration's positions, and so we agree with those.

The one thing that I would note that is important to us and has been talked about a little bit and Senator Franken's question really got to about China is an international presence, but not just a presence of our law enforcement agents, which we in the FBI have and CBP will have, but international training and capacity building.

With the Department of Justice and CBP, we recently undertook to train Chinese investigators, and there is not just lip service from these investigators. They really do want to do some good work, but they really do need that the government, and that is important to us as a law enforcement agency to have partners that have the capacity to work with.

Senator GRASSLEY. The same three people, because we have a finite number of resources for prosecution and for law enforcement, and yet we are seeing piracy and counterfeiting skyrocketing, and even online, do you think that the right holders' actions can alleviate some of the burden on federal law enforcement and effectively combat IP theft?

Ms. ESPINEL. First, I would say we are aware that we have limited resources and an enormous problem on our hands. So part of what my office in coordination with all the agencies here at the table have been working on is how to use those limited resources as efficiently and as effectively as possible. But I think absolutely the private sector has a role to play here. Right holders have a role to play, and I will maybe ask my law enforcement colleagues here to speak a bit about how they interact with the private industry and how the right holders can help support them in bringing cases.

In addition to that, as I mentioned before, I think there are companies that are involved in facilitating Internet commerce, and they can be enormously helpful as well in helping us try to stem online infringement.

Senator GRASSLEY. Mr. Weinstein.

Mr. WEINSTEIN. Senator, I would say that as a general matter, recognizing that we have limited law enforcement resources, all of us do, and that IP crime is a little bit unusual in that it is an area of the law where victims actually have substantial resources typically to enforce their rights, we generally do support giving private parties the tools they need to enforce their rights. We think it is an important complement to law enforcement's ability to focus on the worst of the worst.

To the last thing Victoria said, I think she is absolutely right that we have made relationships with and outreach to industry a priority, all of us have, and one of the things that the IPR Center has done exceptionally well under the really outstanding leadership of Bob Rutt, its current director, who is here, and the folks that Gordon has placed out there is to be a one-stop shop for industry to learn about how to report IP crime and to be kept apprised of what law enforcement is doing and trends in IP crime, and perhaps I will defer to Erik and let him talk about that a little bit more.

Mr. BARNETT. Senator, the question I think is a good one in terms of what government can do. As a public servant for now almost 20 years, I am very proud of what government can do, but, quite frankly, I also recognize government cannot do everything

and is not responsible to do everything. So I think a lot of the work of the private sector is important, and I think what Victoria has tried to do is get those voluntary actions by the private sector so that, frankly, we do not have to pick up a lot of the criminal investigations. So we would support what the private sector can do.

Senator GRASSLEY. Thank you.

Senator WHITEHOUSE. Thank you, Senator Grassley.

Well, we are now down to kind of a murderers' row of prosecutors here for you, and what I would intend to do is recognize first Senator Blumenthal, who served for many years with great distinction as the Attorney General of his home State of Connecticut, and then although I am next, since I have the gavel I will have to be here until the end, then I will yield to Senator Klobuchar, a very distinguished district attorney, a prosecutor from Minnesota, and then I will close out myself. So first, Senator Blumenthal.

Senator BLUMENTHAL. Thank you. Thank you, Mr. Chairman. And thank you for your great work and your testimony today. I have a number of questions, and I suspect that we will not reach all of them, so I would appreciate answers in writing, assuming that we do not.

First of all, to expand on the answer you have given on the private right of action, I would like to know the administration's position on according a private right of action and a greatly enhanced, much more robust one than they may have now. In light of the answer that you have given, Ms. Espinel, about turning up the volume, I would appreciate a specific position on it, and I hope it will be in favor of it because I think in light of the resources that right holders can bring to bear and the need for that kind of enforcement, there is a real opportunity to enhance enforcement through private rights of action.

Second, in terms of the Kohl bill, I am delighted that you are supporting it. I, too, will be joining in it, but a question for you, Ms. Espinel. In light of your very distinguished background in the trade area, isn't there more that we can do to enforce our existing rights as a Nation but also perhaps enhance provisions that are in trade agreements to protect intellectual property?

Ms. ESPINEL. I will mention a few things with respect to international agreements. Probably first and foremost is the international IP agreement that governs all the WTO members is something called the TRIPS agreement, and the TRIPS agreement is an excellent agreement, but it is now 15 years since the TRIPS agreement was negotiated and concluded, and TRIPS was negotiated in a very different world than the one that we face today. So online, I mean, the Internet—you know, it was essentially concluded in the early 1990s when the Internet was not the presence that it is today, and the problems that we are facing in terms of online infringement in the copyright world but also with respect to the health and safety issues simply did not exist. The level of sophistication of counterfeiting, the organized criminal enterprises that Jason referred to, those also did not exist.

So that international agreement does not address those issues because they literally did not exist at the time the agreement was negotiated, and that is the principal reason why the United States, working with Japan and a number of other countries, embarked on

negotiations for an international agreement that would focus just on enforcement, on counterfeiting and piracy, because we knew that the international rules that existed were not adequate to address the challenges. Those negotiations were concluded in November. I think that agreement, the anti-counterfeiting trade agreement, will be of enormous importance as countries sign on to it and it goes into effect, both in terms of increasing cross-border enforcement action but also in terms of setting a new legal standard around the world.

Now, that agreement is not part of the WTO, and while there are 38 countries that have signed on to it and those 38 countries represent half of global trade. China is not yet one of those countries, and obviously from the United States' perspective, we think it is enormously important for China to be there. I think we are hopeful that as more and more countries sign on to that agreement and start increasing standards, China will eventually join.

Senator BLUMENTHAL. Thank you for that answer, and I would appreciate also in writing any additional measures that you think we can take in terms of enforcement, but also perhaps in some of the bilateral areas. As you know, the Senate may soon be called upon to consider trade pacts with Korea, Panama, and Colombia. I would appreciate your views on that one as well.

Ms. ESPINEL. I would be happy to, and I would just say briefly that I think the intellectual property provisions of those agreements are excellent and would be enormously beneficial to the U.S. economy if they went into force. But I would be happy to answer in more detail any questions that you have.

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

Senator BLUMENTHAL. Thank you. Let me also pursue an area with you and other members of the panel because it is mentioned in your testimony in terms of the United States contracting with companies that may be involved, either knowingly or not, because of the supply chain of products that reaches them, particularly in the defense area, where I think there is a vulnerability. As a member of the Armed Services Committee, I would be very interested in your views, again, because we may run out of time here, in writing if necessary on what more the Department of Defense and the Congress can do to prevent the infiltration or entangling of our supply chain with counterfeit or pirated products.

Ms. ESPINEL. Could I speak to that briefly?

Senator BLUMENTHAL. Absolutely.

Ms. ESPINEL. Obviously, it is a very important problem that we are facing. We have been working with DOD and NASA on coming up with a whole series of recommendations, and we set ourselves—we committed ourselves to get those recommendations to the President by early fall. That process is underway, but I strongly suspect that some legislative or regulatory changes may be coming out of that process, so we may be coming back to Congress to ask for your help in terms of those legislative changes. And beyond legislation, there is a whole sort of host of other regulatory policy issues that we feel we need to improve inside the U.S. Government to keep counterfeits out of our supply chain.



The second thing that I would mention is increased law enforcement efforts, and that I would mention not just the work that all of these agencies have been engaged in, but specifically the campaign that Erik mentioned in his opening statement, I believe, that is specifically targeted at prosecuting those who are selling into our military.

Mr. BARNETT. And just to follow up, it was in my written statement as well as my oral remarks. That is, I think—the most important thing about it is that there are nine agencies involved in that, which are the military investigative agencies, CBP, FBI, of course DOJ, as well as the General Services Administration Office of Inspector General. And it is the first time that we have taken a coordinated law enforcement approach to securing the DOD supply chain as well as the federal supply chain, both for obviously the safety of our warfighters as well as, frankly, the taxpayer dollars. So we expect to have vigorous and increased activity over the next six months to a year on that.

Senator BLUMENTHAL. Well, I know you mention in your testimony, a number of you, operations that have been successful—Operation Network Raider, Operation Chain Reaction. But the success of those operations may indicate the need for even more enhanced law enforcement activities in this area because, obviously, there is a problem, and the numbers of dollars, the volume and the magnitude of work are so huge, as you well know, that I think that greatly increased activity may have a lot of payoff.

Thank you.

Senator WHITEHOUSE. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much. Thank you, Mr. Chairman, for holding this hearing, and I know firsthand how important protecting intellectual property is. My State was built on it, everything from the medical device industry to the Post-it note—he is waiting for me to say “Post-it note”—to a lot of our creators in our State from Prince to the Coen Brothers. We are a hot place for new bands, and so all of this intellectual property has led to one of the reasons our State has one of the lower unemployment rates in the country at 6.6 percent. It still not perfect, but without this kind of creativity and thought, things would be a lot worse.

So I am very focused on how to protect that intellectual property, and I think the figures I have seen, we lose something like \$600 billion a year to people, whether they are in China or they set up shop as organized crime to steal our intellectual property. And that is one of the reasons, based on things I was hearing from our own State, whether it is orchestra members or kids working in lighting departments, that they all get hurt when you have this theft, wholesale theft of intellectual property. So that is why I got involved in introducing this bill, and as we all know, it went through the Judiciary Committee without objection, although we know there is some work that needs to be done really in two areas. One is with the cable industry has some concerns and then, second, really to make sure that it is very clear that this is about people who are profiting should be prosecuted. In fact, the statute's exact phrasing, we are actually including this penalty within an exact statute that is already on the books that makes it a misdemeanor,

that it has to be for purposes of commercial advantage or private financial gain.

So I would start with you, Mr. Weinstein, to talk about how this bill does not criminalize any new behavior. It simply takes particularly egregious acts that already actually are considered misdemeanors and makes the worst of the worst subject to felony liability. So could you describe just looking at the felony streaming bill, which, as I said, passed through the Judiciary Committee, how it would not involve—I am looking at some of the blog postings on this, which are very hard to respond to. It would not involve a kid putting a recording of them doing karaoke when they do not do it for profit on the Web. It would not involve a teenager putting some music—a video of a party—this is one today—that includes background music when they are not profiting from putting that video out. It would not include a kid putting their high school band concert on the Web when they are not profiting, and some of these other things that we are seeing that are examples, which have nothing to do with for-profit activity that we are trying to focus on here.

Mr. Weinstein.

Mr. WEINSTEIN. Senator, depending on how bad the band is, it may be a crime to post it online.

[Laughter.]

Mr. WEINSTEIN. I want to thank you and Senator Coons for your leadership. I know this is an issue that—

Senator KLOBUCHAR. And Senator Cornyn as well.

Mr. WEINSTEIN. And Senator Cornyn as well. It has been an important one for you, and as you know, we have been working with your staffs to provide technical assistance on the bill and are happy to continue to do that.

We agree, I think as a number of us have mentioned, that streaming is a serious and growing problem. It is in some ways the next frontier of online piracy, and it is one that the content industry is greatly concerned about.

To answer your question, we are still reviewing the bill, but based on my understanding of what it says, my answer to your question, “Does it make anything criminal that is not currently criminal?” is no, with one limited exception. For the most part, it takes conduct, as you said, that would be a misdemeanor and just makes it a felony, which we think is a more appropriate treatment given the seriousness of the crime and the impact that it has economically.

The exception is for the streaming of pre-release works. Currently, to be a misdemeanor, to stream a pre-release work and have it be a misdemeanor, it would have to be for commercial purpose or private financial gain. Under the bill, as I understand it, pre-release streaming would become a felony—as is the case, by the way, with distribution and reproduction even if there is no commercial purpose and private financial gain. Now, let me break that down a little bit.

As a practical matter—the blog postings are a little bit off the wall. As a practical matter, any streaming site—

Senator KLOBUCHAR. You are going to be quoted for saying that.

Mr. WEINSTEIN. I am sure I will. I do not think they are any fan of mine, either. But as a practical matter, any site that is going to get prosecuted is one that is going to be with a commercial purpose or for private financial gain, and the way that is defined in the law is really quite broad. If you have an ad-supported site, even if you are not charging for the stream, you are conducting it for a commercial purpose.

The kind of sites that we are interested in, the kind of sites that the content industry is worried about, the kind of sites that are having an economically devastating impact are those that are conducted for a commercial purpose. The irony is that pre-release streaming is probably the most serious and has the most potentially economically devastating effects because streaming pre-release works is streaming them when they have their greatest commercial value, and it is the pre-release streaming, when Congress changed the statute you are referring to to make reproduction and distribution of pre-release works a felony, you did so without requiring the commercial purpose and private financial gain component to it because of the significance of and the economic consequences of pre-release distribution and reproduction. And we think that streaming should be treated the very same way.

So with that limited exception, that pre-release streaming now becomes a felony even without the commercial purpose or private financial gains, you are absolutely correct, although I would add that that is perfectly appropriate and we fully support it.

Senator KLOBUCHAR. Does anyone want to add to this in terms of how you think it would be helpful?

Ms. ESPINEL. I would just say briefly I think to echo what Jason said, streaming is sort of the next frontier, and streaming essentially is just another form of distribution, the way more traditional forms of distribution are. So we think it is completely appropriate to make streaming a felony, distribution by streaming a felony the way distribution of physical copies would already be a felony.

We are going to continue to face challenges as our law sort of sets in place and as the technology moves quickly and often ahead of how quickly we can make legislative changes. But this area of illegal streaming is a place where we already know that we have a problem, and so I think it is enormously important to try to clarify what is essentially an ambiguity or deficiency in our law so that streaming by distribution is a felony as well.

I think there is a misunderstanding, at least from what I have read on blog posts, about what this legislation would accomplish, so I have seen similar sort of anecdotes, someone playing guitar on a street corner takes a video of themselves and posts it, or that this is going to be used to go after individuals, and, of course, that is just simply not true. The purpose of this law, the purpose of our recommendation and the legislation that you introduced, as I understand it, is to essentially make streaming, distribution by streaming, a felony the way that traditional forms of distribution have been for many years.

Senator KLOBUCHAR. When it is for a commercial purpose, because, remember, people think of streaming in other ways. Some of these examples, when you just say that it is a felony by streaming, then they are, like, "Well, anything I put on there, I guess,

then, is a felony.” And that is not what we are saying. And so we will continue to work with people, but I just refer them to the statute that says it has to be for a commercial purpose, with that one limited exception, and for private financial gain.

Thank you very much, and we will continue to work with you and try to get at some of these concerns that have been raised about the bill, and people have to remember that right now someone could be prosecuted for a felony when they are standing on a corner and sell over \$2,500 worth of DVDs, but they cannot be prosecuted for doing the same conduct on the Internet, and that is what we are trying to get at to protect the intellectual property in this country.

Thank you very much.

Senator WHITEHOUSE. Thank you, Senator Klobuchar.

Let me start with Ms. Espinel. You have mentioned this already, but I just want to emphasize that we are here with a lot of people from law enforcement. We are talking about a very significant crime. We are talking about a crime that has colossal economic impacts on our country. And yet there is a very, very mixed message because if you go to a rogue Web site that is hosting this criminal enterprise, you are taken there by legitimate American corporations like Verizon and Comcast that run the network to connect you; you find the places by going to legitimate American corporations like Google and Yahoo! whose search engines will take you to a pirated movie. When you get there, you find legitimate American corporations like MasterCard and Visa processing payments for the rogue Web site. You often find a broader array of legitimate American corporations advertising on those Web sites. So if you are an ordinary American citizen, you are hearing from all of you folks, “This is a serious crime; we really need to do something about it.” But the other message that you are hearing is, “This is perfectly normal. Your ISP will connect you to it. Your search engine will let you find it. Your credit card company supports it, and regular companies that you see all over the place are advertising on it. This must be legit.”

And I do not know why it is that the private sector has not been more energetic about sorting this out amongst themselves, why it is that the content providers, who are themselves very big legitimate American corporations, are not taking stronger action to stop ISPs from providing these connections, search engines from providing the locations, and credit card companies and advertisers from supporting the rogue Web sites.

What is your insight into that? And what can we do to accelerate that process? Because we can talk until we are blue in the face about what a big crime this is, but when every signal the ordinary consumer gets from this is this is legitimate, all these companies that I know and like and are part of the American economic landscape are in on the deal, this cannot be bad.

Ms. ESPINEL. So first I will start off by saying I completely agree with you, and that is the reason why we have been so focused on getting all the different types of companies that you named, every single one of them, more engaged and taking voluntary action in this process. And that process is still underway, and I agree with you that we certainly would like to see it move much more quickly,

although we also want there to be private sector not just engagement but enthusiasm about this process, and so that takes some time.

I would like to mention that—you talked about credit cards and payment processors. In my view, the major credit card and payment processors have stepped up. We have very recently come to agreement on a set of best practices that I think could have a significant impact on infringement, and there is a—we will be reviewing how that works, and six months from now, I hope that we are in a position that we will be able to report some real progress there in terms of cutting off these illegal sites' ability to sell their goods.

But we are also in discussions with the advertisers, as you mentioned. We are in discussions with the ISPs. We are in discussions with the search engines. They are all different parts of the Internet economy, and we have made it very clear to all of those parts that we feel that they all need to be there, that this is also not just a problem for credit cards or just a problem for the ISPs or just a problem for the search engines. We really need to have all the parts of the Internet ecosystem working together if we are going to be effective.

This is criminal activity, and nothing is going to be entirely effective. Criminals are always going to look for ways that they can evade law enforcement and that they can evade what the private sector did. But we do feel strongly that if we have both increased law enforcement—and I hope that it has been clear through everything that has happened in the past year how serious our commitment is, but combined with that increased voluntary action from the private sector, I think that can make a tremendous difference. But we need to have all the parts of the ecosystem that you mentioned, we need to have everyone working together.

Senator WHITEHOUSE. Mr. Weinstein, aren't those other parts of the ecosystem actually as a matter of law aiding and abetting the criminal enterprise in supporting it in these different ways?

Mr. WEINSTEIN. Well, Senator, as you know, I think the law on secondary liability civilly is trending away from that conclusion; that is, it is increasingly difficult even in the civil context to hold some of these companies accountable without being able to establish that they specifically took steps to make the infringement succeed. And that is certainly amplified in the criminal context where you have got a higher burden of proof and a willfulness standard.

So I think that if a company that is facilitating infringement without knowingly facilitating infringement, willfully doing it, intentionally trying to make it succeed, I think that it is quite difficult to make a criminal case. That is not to say that there are not a set of facts that would support it, but I think—

Senator WHITEHOUSE. Well, let us talk for a minute about civil cases. Sometime ago Microsoft brought a very effective civil case to shut down the Waledac botnet. The Department of Justice and the FBI were very effective recently with a legal action, a civil action, that shut down the Coreflood botnet after, I do not know, over hundreds of millions dollars, I think, in damage had been done. I forget the exact number that was used in our briefing.

In some cases, it appears that both the ISPs and the search providers, they are happy to participate; they just do not want to have

to do it on their own and be the actor against these sites. They prefer, it seems sometimes, the legal protection and the security and the assurance of a court order that somebody obtained that said you must shut down access to this site.

Why is there not more of that going on? You would think that you could almost have a friendly lawsuit between the content provider and the ISP where they go into court together, they agree, much in the way that happened with the Waledac botnet with Microsoft. There was no real opposition there. It was just a question of sorting it all out, going before the court, getting the order, and the next thing you know the botnet is shut down. Why can't that apply with respect to rogue Web sites as well?

Mr. WEINSTEIN. Well, civil enforcement is not my area of expertise, but as I think some of the cases you mentioned, in the lime wire case and some others indicate, we have not found some of the companies, the rights holders, at least, to be shy about resorting to their civil remedies when they think that they have got a case.

I do not know why there are not more of these sort of friendly lawsuits that are designed to get court orders that give companies cover. You know, Victoria, I think, has been exercising tremendous leadership in trying to bring these companies together voluntarily, as she talked about, and she is too modest to say it, so I will. I do not think that any of that process would be happening if her office did not exist and if she was not in it.

She may have a better insight into sort of what their thinking is about how to balance their need to avoid liability with their concerns about what their customers will think if they are assisting law enforcement or appearing to be anti-free Internet. So she may have a better window because she has been participating in the discussions about what their thinking is. But I do think it is very encouraging that they are taking the voluntary steps they are talking about that she has been discussing.

Senator WHITEHOUSE. Well, we will come back to that. One of the nice things about waiting to go last is that I have nobody waiting and I can go over my time.

The question of resources I think is a significant one, and I know that you all are somewhat constrained by OMB in what you are allowed to say about your need for resources. But let us just talk about these cases in terms of their complexity.

As I understand it, if you want to be really effective in this area, you need to combine not only traditional criminal prosecution with these very modern, Coreflood/Waledac-type civil actions that can help shut down the criminal activity. Rather than just try to find somebody guilty of it and find them and punish them, you can actually stop it. It tends to be international, which makes for exactly complicated investigative and prosecutorial issues dealing with foreign jurisdictions. It tends to have very considerable technical complexity that a prosecutor and an agent have to understand in order to investigate it.

When you put it all together, it strikes me that these are really apex cases in terms of resource intensiveness and complexity. Is that your experience as well? That is a question for Mr. Snow and then Mr. Weinstein.

Mr. SNOW. Yes, sir. These cases tend to be very complex. Some of the lower-level cases that we had maybe in the past decade or so, when we talked about the physical seizure of goods in the marketplaces and on the street corners were a normal investigative case. It relied on almost the drug analogy-type drug case, drug-trafficking resource model, whatever was needed in order to secure the area, to grab the goods, and then come back for the search and the normal prosecution.

Now that we add the Internet into it, it goes in that exact same venue that you are talking about. Huge forensic capabilities are needed to look at the evidence that is seized, the evidence that is taken down, and how we actually in all realms on the Internet and in cyber cases deal with anonymization and movement through to actually find out who is behind this act itself. So everything—

Senator WHITEHOUSE. Particularly where the activity is originating overseas and it makes the investigation extremely complicated to be operating in a foreign nation.

Mr. SNOW. Yes, sir, absolutely. And then the same side—and I will let Jason talk for himself, but the same side with the CHIPS attorneys and the DOJ prosecutive process.

Mr. WEINSTEIN. You will recall in April Mr. Snow and I were here talking to you about cybersecurity and cyber crime, and I think you made a very similar observation about cyber and intrusion cases. And everything you said then and everything you have said today applies with equal force to these IP cases.

I just want to highlight one thing that Gordon said, which is forensics. You know, the cases are complicated enough when you are talking about collecting electronic evidence, but they place a significant burden on very, very limited forensic resources. You know, computer forensics is a concern in every type of case, but it is a particular concern in cyber and IP cases.

So these are incredibly resource-intensive cases, and the cases that are likely to have the greatest impact are the ones that are the hardest and the most expensive.

Senator WHITEHOUSE. A number of you have discussed sales to the military as an area of particular concern in terms of counterfeiting. I know we have had cases in which the Kevlar was not Kevlar or in which the advanced microchip was not an advanced microchip. And, of course, anything that puts our soldiers and the equipment that they need at risk is of particular importance.

Senator Coons and I have a bill on our side, joined by Senator Graham and Senator McCain on the other side, to increase the penalties for military counterfeiting, and I would appreciate if each of you could give your reactions to that bill, anything in the way of technical assistance or recommendations that you would make. And I think probably based on your position, Ms. Espinel, if you are in a position to say that the White House would support it or not, or with changes, that would be helpful. It is a bill we would like to move, and we would like to make sure it is well supported. I think it is already strongly bipartisan. It makes a lot of sense. A number of you have already raised the issue today, so there is a lot of potential here. I would like to make sure it happens, and I would like to get your reactions to it as a question for the record, if I may. If you would like to respond briefly now as well, but I do

not want that to constrain a written response in a question for the record.

Ms. ESPINEL. We would also be happy to send a written response, but I will just say briefly, as you know, we made recommendations to Congress in March to increase penalties, increase the Sentencing Guidelines for sales to the military. It is an enormously important issue. We were very pleased to see the legislation that was introduced. As it was recently introduced, we are still in the process of assessing it. But I think I can speak for DOJ or at least ask DOJ to confirm that we would—my office would certainly be happy to work with DOJ on technical assistance on the legislation, and we think it is very important.

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

Mr. WEINSTEIN. I completely agree. We have been working with your staff for a while to provide technical assistance, and we are obviously happy to continue to do that. We think it is a very important issue, and it demonstrates more than anything that IP crime can be a national security issue. Anybody who thinks that IP crime is just selling a bunch of DVDs and counterfeit Nikes on the street should read a description of one of these cases involving a counterfeit network hardware that was going to be used in a computer system to control troop movements in Iraq. It will make your jaw drop. IP crime is a national security crime, and we think this is a vitally important issue to pursue.

Senator WHITEHOUSE. Very good. I guess the last thing I would mention before I let everybody go at the noon hour is that I am a member of the International Anti-Piracy Caucus, along with Senator Hatch. The Caucus has highlighted China as one of the watchlist countries that fail to protect American intellectual property. From my time on the Intelligence Committee, there is other information out there that this is not an appropriate forum to discuss in, but a great deal of the public information that has come out about the major attacks and hacks on corporations and infrastructure has traced that back to China. China appears to be the most dangerous and active nation state actor, malefactor, in this area, and the administration has recently signed a letter of intent with China's Ministry of Public Safety on law enforcement cooperation in this area.

Given the extent to which not only in this behavior seeming to emerge from China, but it often seems to be sanctioned—the example I have used is in the old days privateers were put on the ocean and they were allowed to attack other ships if they had letters of mark from a country or principality. They were essentially private actors, but they had that going on behind them. And I think that it appears that a lot of the activity coming out of China is basically privateers who are operating with knowledge and the implied consent perhaps of the government. Certainly it is a significant economic transfer of wealth into China from our country.

How will you ensure that the relationship with China's Ministry of Public Safety will be productive going forward given the mixed messages, shall we say, we are getting from this country?

Mr. SNOW. Sir, I will go ahead and take that question, and I would just state that we spent some time with the Director of Intel-



ligence, and we spent some time sending an agent over there TDY to Beijing not only to look at a lot of things that were going on in the Intellectual Property Rights Center but to feel out that relationship with MPS. I think Mr. Barnett pointed to it earlier, that MPS is very forward leaning in trying to address the threats that they may have over there, as well as for us to engage in a good conversation and discussion on the threats that we see emanating trans-border into the United States from China.

So we are hoping—and I think it will be fruitful—that that direct connect that we will have with the FBI, with Customs and Border Protection in the future, with ICE, will be that original ground-breaking initiation that it takes in order for those law enforcement officers to actually take a look at the threat and provide the information that all countries need to do to address this globally.

I think we see that in many respects across the world as history developed itself, but I am hoping that that is what we will see as we move with MPS.

Senator WHITEHOUSE. Well, I would encourage you to participate in this and to pursue it. But I do not need to tell you that you need to do so guardedly given the issues on the other side. Senator Klobuchar mentioned this with respect to Minnesota. Rhode Island does a lot of invention and design. The Rhode Island School of Design is one of the legendary universities in this area. I have spoken to Rhode Island manufacturers who have been invited to open plants in China, and they have refused to do so because it is their expectation that the purpose of that invitation was to give access to their technology, to their procedures, to their intellectual property in ways that would allow it to be stolen, instantly reproduced, and they would find a competitor fully up to speed with their technology but not paying them any licensing fees or anything for the effort and the expense that they put into developing the technology. So, you know, right down to a local manufacturer in Cranston, Rhode Island, the concern about what China is doing to our intellectual property is a very real, immediate, and grave one, and I hope that continues to be a significant issue for the administration not only in law enforcement but also as we deal with them in the diplomatic and trade venues. It seems to me that it—I have said that we are on the losing end of the biggest transfer of wealth through crime and piracy in the history of humankind, and we need to do a lot more about it. I know that each one of you is doing an enormous amount about it in your own offices and in your own ways, and I thank you for your time this morning, and I thank you for your service to our country in this important cause.

The record of the hearing will remain open for an additional week if anybody wishes to add anything, and unless there is anything else to put into the record—no, there is not—we will stand adjourned. Thank you all very much.

[Whereupon, at 12:03 p.m., the Committee was adjourned.]



## **A P P E N D I X**

### **ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD**

Witness List

Hearing before the  
Senate Committee on the Judiciary

On

“Oversight of Intellectual Property Law Enforcement Efforts”

Wednesday, June 22, 2011  
Dirksen Senate Office Building, Room 226  
10:00 a.m.

The Honorable Victoria A. Espinel  
Intellectual Property Enforcement Coordinator  
Office of Management and Budget  
Washington, DC

Jason Weinstein  
Deputy Assistant Attorney General, Criminal Division  
U.S. Department of Justice  
Washington, DC

Gordon Snow  
Assistant Director, Cyber Division  
Federal Bureau of Investigation  
Washington, DC

Erik Barnett  
Assistant Deputy Director  
U.S. Immigration and Customs Enforcement  
Washington, DC

Allen Gina  
Assistant Commissioner, Office of International Trade  
U.S. Customs and Border Protection  
Washington, DC

## PREPARED STATEMENT OF CHAIRMAN PATRICK LEAHY

**Statement Of Senator Patrick Leahy (D-Vt.),  
Chairman, Senate Judiciary Committee,  
Hearing On "Oversight Of Intellectual Property Law Enforcement Efforts"  
June 22, 2011**

I thank the witnesses who are here today to discuss the enforcement of our Nation's intellectual property laws. This is an issue on which this Committee has focused a great deal in recent months, and there is good reason for it. While estimates of intellectual property theft are difficult to quantify, reports indicate that it costs the American economy billions of dollars and hundreds of thousands of lost jobs. This is unacceptable in any economic climate, and it is devastating today.

Whether intellectual property theft takes place on street corners or on the Internet, it poses a threat to American businesses, American public safety, and even the American military. This problem, simply put, is an epidemic. Thanks to the work of each of our witnesses, however, it is one that we are making significant strides to combat.

Today's hearing is almost a year to the day from our first oversight hearing for the Intellectual Property Enforcement Coordinator (IPEC) position, which was created by the PRO-IP Act. Several members of this Committee cosponsored that bill, and one of the primary motivations behind creating this new position was to have one central presence to coordinate the work being done across the Government to combat intellectual property theft. This is why today, it is fitting that the IP Enforcement Coordinator Victoria Espinel joins us, again, and that she is joined by representatives from some of the key enforcement agencies with which she works, the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), Customs and Border Patrol (CBP), and Immigration and Customs Enforcement (ICE).

I am pleased with the work that your agencies have done together to combat intellectual property theft in the short time since the creation of the IPEC position. All of your agencies, as well as the other members of the Intellectual Property Rights (IPR) Center, deserve credit for putting egos and turf aside, and coordinating your investigative and prosecutorial efforts for the larger goal. I know there are times where each of you has had to defer to another agency in pursuit of a high-profile investigation. That is not always easy, but we are better off as a result.

Ms. Espinel, last year when you appeared before this Committee, you unveiled the IPEC's Joint Strategic Plan against counterfeiting and infringement. That plan outlined the general purposes behind your intellectual property enforcement strategy, which included growing the American economy, promoting innovation, protecting consumer trust and safety, and preserving our national security. Since that time, the agencies appearing here today have made strides towards these ends.

Two areas in particular stand out. The first is criminal enforcement. Over the past year, the coordinated efforts of the Justice Department and law enforcement have resulted in victories in several high-profile criminal infringement suits, including two cases involving more than \$100 million in counterfeit merchandise. The Justice Department and ICE also ran a successful

“Operation In Our Sites”, which has resulted in the takedown of more than 120 domain names of websites that were trafficking counterfeit goods.

The second advance is your ability to engage so many prominent members of the Internet “ecosystem” – including payment processors, Internet registrars and ad networks - to come together voluntarily to combat online infringement. This complements the work we have been doing in Congress on the PROTECT IP Act, which would require these same third parties to stop doing business with an Internet site that a court determines is dedicated to infringing activities. I applaud these voluntary activities, such as the recent non-profit formed to crack down on illegal online pharmacies. The private sector can always do more to self-police than the Government could ever enforce on its own. We need to work together to successfully combat online theft.

You should all know that your work has the support of this Committee. While there are many issues in which our members have spirited disagreements, the protection of intellectual property is not one of them. Intellectual property enforcement is a great example of a bipartisan area where this Committee has come together to report meaningful legislation. The PRO-IP Act, for example, was cosponsored by 22 Senators, 11 Democrats and 11 Republicans, and it passed the Senate unanimously. Similarly, last month we reported the PROTECT IP Act unanimously from this Committee, and the House is currently considering another IP-related bill, the America Invents Act, legislation that passed the Senate by a vote of 95-5.

There is a long way to go to combat the problem of intellectual property infringement, but you have accomplished a great deal in a short time. Ms. Espinel, your plan represents a way forward to a stronger and more effective enforcement effort, and I thank you for your efforts.

I look forward to hearing the testimony of all witnesses today.

#####

PREPARED STATEMENT OF HON. VICTORIA A. ESPINEL, INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, OFFICE OF MANAGEMENT AND BUDGET, WASHINGTON, DC

EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

Testimony of Victoria A. Espinel  
Intellectual Property Enforcement Coordinator, Office of Management and Budget  
Before the Committee on the Judiciary  
United States Senate  
June 22, 2011

Chairman Leahy, Ranking Member Grassley, members of the Committee on the Judiciary: Thank you for your continued leadership on this important issue. I also want to thank you for the support that this Committee has provided to my new office and the Administration's overall efforts. Although my new office is very small and operates with extremely limited resources, your support and the attention you bring to this issue has helped us to be more effective.

One year ago today we sent to you the Administration's Inaugural Joint Strategic Plan on Intellectual Property Enforcement. That Strategy was developed with significant public input -- including more than 1,600 comments from the public -- and the coordinated efforts of the Federal agencies, including the U.S. Departments of Commerce (DOC), Health and Human Services (HHS), Homeland Security (DHS), Justice (DOJ), State and the Office of the U.S. Trade Representative (USTR). The overarching goal of the Strategy is to protect U.S. jobs, to increase exports of innovative technology and creative works and to support and protect our innovation, thereby allowing America's innovation to continue to drive our economic growth. A second principal goal is to protect the health and safety of the public. One year ago, we set out six broad principles that we would follow to meet our goals and 33 specific actions that we would take to improve enforcement. We knew the Strategy would take far more time than a year to fully implement, but we are making progress and I want to highlight some of the concrete steps that we have taken to support those principles and to improve enforcement since we issued the Strategy a year ago.

**I. Lead by Example**

First, we will lead by example and work to ensure that the U.S. Government does not purchase or use infringing products. On January 7, the U.S. Chief Information Officer, the Administrator for Federal Procurement Policy and I issued a statement to Federal procurement officials reminding them of the Administration's policy to be "technology neutral" in procurement, and that all

technology must be properly licensed. We are also reviewing our policies with respect to use of software by our Federal contractors.

We must prevent counterfeit and pirated products from coming in to the U.S. Government supply chain and take aggressive action against those who sell them to our military and other critical infrastructure. We are working closely with the Department of Defense, National Aeronautics and Space Administration, DOJ, DHS and other federal agencies on stopping counterfeit and pirated products from entering the U.S. government's supply chain, particularly our military and critical infrastructure, and taking aggressive action against those who are selling such products. *Operation Network Raider* is a collaborative interagency law enforcement initiative that aims to end the illegal distribution of counterfeit network hardware manufactured in China. The results are compelling: 30 felony convictions and over 700 seizures of counterfeit Cisco network hardware valued at more than \$143 million. In addition, U.S. Immigration and Customs Enforcement (ICE) has recently initiated – in coordination with nine of its National Intellectual Property Rights Coordination Center (IPR Center) partners – *Operation Chain Reaction* to prevent counterfeits from entering the U.S. government's supply chain.

## **II. Transparency**

Second, we will be transparent in our policymaking and enforcement. We have and will continue to meet with a wide range of stakeholders as we implement the Strategy. Federal Bureau of Investigations (FBI) and ICE have also increased the transparency of government efforts to protect intellectual property by conducting outreach and developing education programs for industry representatives with a stake in intellectual property enforcement.

## **III. Improve Coordination**

Third, we will improve coordination, including coordination of our law enforcement, the men and women stationed in our embassies overseas and our international training. On February 8, President Obama signed Executive Order 13565 establishing a Cabinet-level intellectual property advisory committee chaired by the Intellectual Property Enforcement Coordinator (IPEC) to further focus our efforts. We now have 30 law enforcement teams across the country, led by ICE or the FBI, that include federal law enforcement and state and local law enforcement to fight intellectual property crime. The FBI has enhanced the coordination of intelligence of global IP threats through its Intelligence Fusion Group, as well as avoiding conflicts of agencies working on IP cases through its Intellectual Property Rights Unit stationed at the IPR Center. Overseas, we identified 17 countries in which improving intellectual property enforcement is a priority. The embassies in each of those countries have each established senior-level intellectual property working groups and have completed detailed plans setting out the actions each embassy will take to address the specific challenges in those countries. We established interagency working groups to better coordinate our training efforts and make sure that our limited resources are used wisely.

As part of this effort, last month, the U.S. Patent and Trademark Office (USPTO) launched a new searchable database ([www.usipr.gov](http://www.usipr.gov)) for U.S. Government intellectual property enforcement training programs conducted around the world. The database will increase transparency, by allowing the public to see how the U.S. Government is allocating resources on intellectual property training; increase public participation, by identifying upcoming training events that are open to the public; use resources more efficiently, by sharing training materials between U.S. Government agencies; and avoiding duplicative programs and improve results, by building on past programs and targeting U.S. Government efforts on countries and topics where more training is needed.

#### **IV. Increase enforcement overseas**

Fourth, we will increase enforcement overseas, including pressing foreign governments to do more to protect American right holders. As of last September, ICE has a full time agent in China dedicated to IP issues. The FBI is also preparing to assign a person to China later this year who will work exclusively on IP issues. Moreover, in the President's 2012 budget, DOJ is requesting funds to place six International Computer Hacking and Intellectual Property Coordinators, or "ICHIPs", in strategic global locations to strengthen international intellectual property efforts. The ICHIP program would also support the DOJ's international organized crime strategy as related to IP, online fraud, and data breaches that threaten U.S. economic security in targeted regions around the world.

We are pressing our foreign counterparts to do more. President Obama, Vice President Biden, Attorney General Holder, Secretaries Geithner and Locke, U.S. Trade Representative Ron Kirk and Department of Homeland Security ICE Director John Morton, U.S. Customs and Border Protection (CBP) Commissioner Alan Bersin, Under Secretary of State Robert Hormats and other senior Administration officials have directly and repeatedly pressed China and other countries to do much more to combat intellectual property theft.

Both Attorney General Holder and DHS ICE Director Morton traveled to China within the last year to press their counterparts for increased cooperation to fight intellectual property crime. This was the first time an ICE director has traveled to mainland China and Director Morton made IP enforcement a major focus of his trip, signing a Letter of Intent with the Ministry of Public Safety on law enforcement cooperation. On May 5, 2011, Director Morton signed a Memorandum of Understanding on law enforcement cooperation with the China General Administration of Customs (GACC). In May, CBP worked with the GACC to increase opportunities for information-sharing for both sides. CBP also signed a Memorandum of Understanding with the Ministry of Public Safety (MPS), which will lay the groundwork for information-sharing and collaboration between the two agencies.

We are also seeing greater cooperation from some foreign governments.



In June, in association with Operation In Our Sites, several U.S. law enforcement agencies worked cooperatively with Dutch law enforcement authorities to seize an image server in the Netherlands being used to facilitate the unauthorized reproduction and distribution of copyrighted material. That same month, the FBI worked with Latvian authorities to arrest and to extradite a trafficker of counterfeit gaming machines and in August, the trafficker and his partner were each sentenced to two years in prison, and ordered to pay \$151,800 in restitution.

On February 24, pursuant to an extradition agreement, U.S. Marshals took a defendant into custody in Paraguay to return him to the United States to face charges, including of the sale of counterfeit goods. The defendant is alleged to have committed his crimes to raise money for the terrorist group Hezbollah.

On January 21, a citizen of Belgium who was arrested in Costa Rica and extradited to the United States, pled guilty to operating an illegal Internet pharmacy that sold \$1.4 million worth of counterfeit and misbranded drugs (along with controlled substances). The defendant used multiple websites to sell more than 40 prescription drugs. He operated a customer call center in the Philippines, received payments from customers using a credit card processor in the Netherlands, and paid employees using Western Union in the Philippines, Costa Rica, and the United States. Earlier this month, he was sentenced to 48 months' imprisonment.

With cooperation from the Mexican Tax Administration Service – one of the IPR Center's foreign law enforcement partners – ICE and CPB were able to help bring about the seizure of 306 tons of counterfeit merchandise at mail facilities and land, air and sea ports of entry in one joint operation, seizing over \$23 million worth of goods.

Under Operation Pangca III the United States targeted online sale of counterfeit and illegal medicines in coordination with 45 countries, resulting in worldwide arrests and seizures of thousands of potentially harmful medications. This is one of three global law enforcement sweeps that the United States has led and participated in since June of 2010, coordinated with the World Customs Organization, INTERPOL, and others, each involving more than 30 countries, targeting counterfeit drugs and online piracy.

And in November, the U.S. Trade Representative concluded negotiations on the Anti-Counterfeiting Trade Agreement with 37 other countries, who together with the United States represent over 50 percent of global trade. That agreement will be the first international agreement focused exclusively on intellectual property enforcement and we hope that the agreement will increase cooperative cross-border activity.

China is clearly a priority focus because of the scope and volume of its problems there. In January, President Obama and President Hu issued a joint statement, agreeing that China will strengthen its efforts to protect intellectual property rights, including by conducting audits to ensure that government agencies at all levels use legitimate software, and that it will not link its

innovation policies to the provision of government procurement preferences. The two countries made further progress in May during the Economic Track of the U.S.-China Strategic and Economic Dialogue (S&ED) led by Treasury Secretary Geithner, including China's commitment to eliminate all of its government procurement indigenous innovation product catalogues and revise its draft Government Procurement Law Implementing Regulations to eliminate the requirement to link indigenous innovation products to the provision of government procurement preferences, as part of its implementation of President Hu's January 2011 commitment. Last October, China launched a nation-wide "Special Campaign Against Piracy and Counterfeiting" (Special Campaign). This campaign has had high-level attention by China's State Council and was led by a Chinese Vice Premier, who coordinated IPR enforcement efforts across China. At the May S&ED, China pledged to improve its high-level, long-term intellectual property rights protection and enforcement mechanism, building on the Special Campaign, and we are working with USTR, USPTO and other federal agencies and with our industry to assess the impact of the Special Campaign and to press China to do more.

On February 28, the U.S. Trade Representative issued a report identifying 30 online and physical markets – including China's search engine, Baidu, and e-commerce platform, Taobao – as "notorious markets," in which pirated and counterfeit goods are reportedly available. The report will help guide the Administration's trade-related enforcement efforts. We have already seen voluntary action from sites listed in the special report, such as Taobao's announcement that it will increase efforts to crack down on counterfeit and pirated products being sold through its system. The Government of Hong Kong has already taken action against a market listed in the report, heightening surveillance and bringing criminal prosecutions at the notorious "Ladies' Market".

Through its Trade Agreements and Compliance Program, ITA's Office of Intellectual Property Rights (OIPR) continued to work with other U.S. Government agencies to help U.S. businesses by suggesting strategies they can take to evaluate IPR problems encountered abroad. Since June 2010, 60 cases were initiated on behalf of U.S. rights holders. Of those, 20 cases were on behalf of U.S. small and medium-sized businesses. Fifteen barriers in 14 countries were removed. OIPR also launched a number of additional tools and services to help U.S. businesses protect and enforce their IPR abroad which are now available through [www.stopfakes.gov](http://www.stopfakes.gov), including a new Transatlantic Intellectual Property Rights Resource Portal launched in December 2010.

And on May 14<sup>th</sup> as the result of close work with France and other European allies, the Group of Eight (G8), released a final declaration that includes strong statements on the importance of enforcement and a joint commitment to protect intellectual property rights, including to take "effective action against violations of intellectual property rights in the digital arena, including action that addresses present and future infringements". The G8 declaration highlighted "the importance of enforcement in order to incentivize innovation and protect innovation once

developed,” and recognized “the need to have national laws and frameworks for improved enforcement.” (emphasis supplied)

#### **V. Secure our supply chain**

Fifth, we will secure our supply chain. That includes securing the physical border, working to minimize infringing products coming into the U.S. and innovative technology from being illegally transferred out of the U.S.

In Fiscal Year 2010, ICE intellectual property investigations opened are up more than 41 percent and arrests are up more than 37 percent, DHS intellectual property seizures are up more than 34 percent, and FBI intellectual property investigations opened are up more than 44 percent.

DOJ has bolstered state and local law enforcement efforts by providing over \$6.5 million in grants, which the program grantees have used to seize over \$195 million worth of infringing merchandise since October of 2009. These seizures are in addition to the increased training, arrests, warrant executions, and other activities that the DOJ grants fund. Specifically, a portion of the funding provides critical training and outreach to law enforcement on effective strategies for intellectual property enforcement efforts. DOJ and the FBI have increased their investigation and prosecution of trade secret cases. Among the examples of cases charged or prosecuted by DOJ last year are two cases involving the theft of technology developed by our automobile industry, including a case involving trade secrets to build hybrid cars. DOJ also prosecuted trade secret cases involving the trafficking of sensitive business practice information belonging to Apple, as well as highly valuable trading software belonging to major financial companies such as Societe Generale and Goldman Sachs. These significant cases are representative of our overall increased enforcement.

Because of serious risks to health and safety, combating counterfeit drugs is a major priority. In March, we sent to Congress a strategy which laid out how we will combat counterfeit drugs sold on the Internet, smuggled into the U.S., and sold in cities throughout the United States. We also have recommended to Congress that it request the Sentencing Commission to increase the guidelines for crimes that pose a serious risk to health and safety. Just last month, for example, an individual was indicted in Pennsylvania for attempting to sell approximately 6,000 boxes of counterfeit LifeScan One Touch diabetic test strips. That same month, a husband and wife in California were sentenced to over three years in prison for selling counterfeit jewelry that contained nearly 20 times the amount of lead deemed safe for children by the Consumer Product Safety Commission.

Securing our supply chain includes not only the physical border, but also combating infringement in the digital world. In the past year, we have advanced a coordinated approach to combat online infringement: increased law enforcement action, voluntary efforts by the private sector and consumer education.

Last June, DOJ and ICE announced the first coordinated effort to target websites engaged in distributing or providing access to pirate or counterfeit goods. Under Operation In Our Sites, American law enforcement has conducted five operations seizing 125 domain names. Over 50 million visitors to these sites were redirected to a banner informing them of the domain name's seizure and of the criminal penalties for infringement.

Effective enforcement against online infringement also requires strong laws that keep up with technology. In March, we made 20 recommendations for legislative changes to Congress to strengthen enforcement. Those recommendations are up on the White House website. Since the release of the legislative recommendations, we have been working with Congress on legislative proposals that reflect the White Paper recommendations. One of those is to make sure that illegal streaming - a form of "distribution" online - is a felony, in the same way that more traditional forms of distribution are.

We know that there is a great deal of interest in Congress in giving our law enforcement additional tools to stop websites engaged in substantial criminal infringing activity. My office has convened a process to develop the Administration's position on this legislation. This is a priority issue for us and we look forward to working closely with Congress to develop effective solutions.

On **engagement with the private sector**, we know that effective enforcement must involve the private sector stakeholders. We are working with private sector companies that facilitate or benefit from e-commerce to encourage practical and effective voluntary actions to address repeated acts of infringement, that respect privacy and fair process and protect legitimate uses of the Internet. Over the last several months, my office has been working closely with Internet Service Providers, advertisers, industry associations, credit card companies, payment processors, search engines, domain name registrars and registries to take action against illegal activity. In January, Vice President Biden held a meeting with Verizon Chief Executive Officer (CEO) Ivan Seidenberg, CEOs from movie, music, software and pharmaceutical companies and representatives of labor and public interest advocacy groups to encourage rapid progress on these types of voluntary agreements.

In December, we announced that American Express, Discover, eNom, GoDaddy, Google, MasterCard Microsoft, PayPal, Visa and Yahoo! had agreed to start a new non-profit to get illegal fake "pharmacies" - actually criminals masquerading as pharmacies- out of their systems and to choke off the revenue that fake "pharmacies" make by preying on the public. The nonprofit will also work on educating consumers on the dangers of buying from fake "pharmacies". In January, the group adopted a name for the nonprofit- the Center for Safe Internet Pharmacies ("CSIP") - and began working on the initial corporate structure and governance documents. By July, CSIP plans to confirm those companies who will serve as

founding members, hire staff to manage the day-to-day operations of the organization, and establish a website.

We need similar efforts on other Internet enforcement issues, including copyright infringement.

Voluntary cooperative solutions are a priority focus and we believe that, in combination with law enforcement action, voluntary actions by the private sector have the potential to significantly reduce online infringement. We are working closely now with credit card companies and advertisers- who do not want to be inadvertently supporting criminal activity- to ensure that infringement will no longer be a profitable business and to cut off revenue for illegal sites. This is illegal activity that legitimate companies do not want be associated with.

The third piece of our online enforcement approach is to make sure the public is aware of the risks of counterfeiting and piracy online. To give just two examples, DOJ is funding public awareness campaigns on the risks to the public of purchasing counterfeit goods and CSIP includes education and public awareness as one of its four guiding principles.

#### **VI. Data**

Finally, we will want to ensure that our policies are built on the best data possible. We are working with the Department of Commerce, the chief economists of the Federal agencies and the President's Council of Economic Advisers on an empirical analysis to identify the industries that most intensively produce intellectual property, and to measure the importance of those industries to the U.S. economy. This is the first time the U.S. Government has ever attempted such a broad analysis across all the sectors of our economy.

As the Joint Strategic Plan described a year ago, the U.S. Government is committed to utilizing the resources at our disposal to improve intellectual property enforcement to grow the U.S. economy; create jobs for American workers and support for U.S. exports; promote innovation and the security of America's comparative advantage in the global economy; protect consumer trust and safety; protect national and economic security; and enforce rights as set out in our Constitution.

I commend this Committee's leadership on intellectual property enforcement and I look forward to working closely with this Committee on improving our protection of American intellectual property.

PREPARED STATEMENT OF JASON M. WEINSTEIN, DEPUTY ASSISTANT ATTORNEY  
GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC



## **Department of Justice**

---

STATEMENT OF

JASON M. WEINSTEIN  
DEPUTY ASSISTANT ATTORNEY GENERAL  
CRIMINAL DIVISION

BEFORE THE  
COMMITTEE ON JUDICIARY  
UNITED STATES SENATE

ENTITLED

**"OVERSIGHT OF INTELLECTUAL PROPERTY LAW ENFORCEMENT EFFORTS"**

PRESENTED

JUNE 22, 2011

Good morning Chairman Leahy, Ranking Member Grassley, and members of the Committee. Thank you for the opportunity to discuss the important topic of intellectual property protection and to share with the Committee the Department of Justice's strong commitment and vigorous efforts to combat intellectual property crime both here and abroad. We appreciate the tools Congress gave to the Department in the Prioritizing Resources and Organization for Intellectual Property Act of 2008, better known as the PRO IP Act, and I'm pleased to discuss how those tools fit within the Department's overall strategy for protecting intellectual property.

### **Background**

As this Committee is acutely aware, criminal enforcement of intellectual property rights is critical to safeguarding our economy and creating economic growth. Effective enforcement creates a level playing field for competition in the global marketplace where American creativity and innovation can thrive. But intellectual property protection is not only important to our economic well-being, it is also indispensable to safeguarding the interests of American consumers. Consumers are entitled to rely on a marketplace that offers safe and legitimate goods. Effective enforcement of intellectual property laws ensures that products are what they appear to be so that consumers know what they are getting; it rewards brand owners who make quality products; and it holds accountable those who manufacture or sell counterfeit goods, particularly products that are second rate, or worse – unsafe.

Protecting intellectual property rights has been a Department priority for more than a decade, beginning in 1999, when then-Deputy Attorney General Holder announced the Department's first intellectual property initiative. I can tell you first-hand that Attorney General Holder is just as concerned about the protection of intellectual property rights today as he was when he announced the initial IP initiative 12 years ago. In fact, he is even more concerned, as the new technologies and globalized economy that have created unprecedented opportunities for innovation and economic growth have also led to unprecedented challenges from the criminal element that we could not have conceived of in 1999 – or even 2009.

We live in a new world with incredible business possibilities for individuals and companies both large and small. The increasing availability of Internet access, and at faster rates, has allowed rights holders – whether a company or an individual -- to distribute or stream digital content to a worldwide market almost instantaneously. Add to that improvements in manufacturing, transportation, and shipping, and even small businesses have unprecedented opportunities to market and distribute their goods and services around the world.

As we all know, intellectual property criminals have exploited these same opportunities to operate illegal enterprises that profit from the hard work of American artists and innovators. They are technologically savvy criminals who have developed equally sophisticated and diverse methods of committing every type of intellectual property offense imaginable, including

widespread online piracy; corporate and state-sponsored economic espionage; increased sales of counterfeit goods, including computer network hardware that can threaten our national security; and increased international trade in counterfeit pharmaceuticals and other goods that pose substantial risks to the health and safety of American consumers.

Moreover, new technology often allows intellectual property criminals to operate anonymously in cyberspace from almost anywhere in the world -- and more significantly, frequently well out of the reach of U.S. law enforcement. They steal brands and creative works from American rights holders, who produce far more intellectual property than any other nation, and then -- to add insult to injury -- they turn right around and sell their fake, unlicensed, and often dangerous goods to American consumers -- hurting our nation twice in the process.

But the story doesn't by any means end there. The good news is that the Department is well up to the challenge. As the sole department responsible for both investigating and prosecuting criminal offenses, the Department is uniquely situated to enforce criminal laws protecting this nation's intellectual property, including those involving copyrighted works, trademarks, and trade secrets. The Department has developed an ongoing robust and comprehensive criminal enforcement network designed to address the increasingly sophisticated, transient and diverse methods of committing IP crimes.

The Department relies on the aggressive efforts of a formidable investigative and prosecution team to combat intellectual property crime, including:

- the 94 United States Attorney's Offices (USAOs) and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS), as well as other components in the Department;
- the Federal Bureau of Investigation (FBI);
- other law enforcement partners, including U.S. Immigration and Customs Enforcement -- Homeland Security Investigations (ICE-HSI) and many other federal law enforcement and regulatory agencies partnered at the National Intellectual Property Rights Coordination Center (IPR Center);
- a growing number of state and local law enforcement agencies who participate in intellectual property task forces around the country; and
- last, but certainly not least, given the transnational scope of IP crimes, our foreign law enforcement partners around the world.

I know the Committee is aware of much of the Department's work from the PRO IP Act Annual Reports that the Department and the FBI have submitted to Congress in fiscal years 2009 and 2010. The 2009 reports covered not only the first year following enactment of the PRO IP



Act on October 13, 2008, but also included a review of the previous five years. As a result, Congress now has received from both the Department and the FBI seven years of intellectual property statistics and detailed accounts of notable cases, major enforcement programs, training strategies, domestic and international outreach efforts, and more. Also, as required by the PRO IP Act, both annual reports included descriptions of the Department's efforts to implement the PRO IP Act itself, which is of course in part the subject of today's hearing. I realize the members of the Committee likely already have reviewed or been briefed on those reports, so I will use my time to highlight only a few of the major components of the Department's overall IP criminal enforcement efforts.

## **II. High-Level Commitment to Intellectual Property Enforcement**

Congress has emphasized with passage of the PRO IP Act that it is critical for law enforcement and other government entities involved in protecting intellectual property rights to design and implement top-level intellectual property enforcement strategies. This is necessary not only to confront the sophistication and global reach of today's intellectual property criminals, but also to make the most efficient use of limited resources. While the Department has long realized the importance of such strategic thinking, we recognize that such efforts have only become more important as the threats to intellectual property have multiplied over time.

### **A. The Task Force on Intellectual Property**

As I mentioned earlier, the Attorney General has made the investigation and prosecution of IP crime a top law enforcement priority. In February 2010, the Attorney General announced the creation of a new Task Force on Intellectual Property (IP Task Force). The IP Task Force is chaired by the Deputy Attorney General and is comprised of senior-level officials from the Office of the Attorney General, the Office of the Associate Attorney General and every Department component with a stake in intellectual property enforcement, including Lanny Breuer, Assistant Attorney General of the Criminal Division; Tony West, Assistant Attorney General for the Civil Division; Laurie Robinson, Assistant Attorney General for the Office of Justice Programs; Marshall Jarrett, Director of the Executive Office for U.S. Attorneys; Zachary Miller, Acting Deputy Assistant Director of the FBI's Cyber Division; and U.S. Attorney Jenny Durkan, Chair of the Attorney General's Advisory Committee's Subcommittee on Cybercrime and Intellectual Property.

The IP Task Force seeks to enhance intellectual property protections by strengthening and providing greater focus on our domestic enforcement efforts; by increasing our international engagement; and by coordinating better with our state and local law enforcement partners. The IP Task Force has guided and provided high-level support for the Department's substantial efforts to combat intellectual property crime.

### **B. Collaboration with the Intellectual Property Enforcement Coordinator**

The Department has also worked closely with Victoria Espinel, the Intellectual Property Enforcement Coordinator (IPEC), a position that Congress established under Title III of the PRO IP Act. Her strong leadership has contributed greatly to the Administration's comprehensive approach to intellectual property protection and enforcement. The Department is a key member of the IPEC's Advisory Committee and has made substantial contributions to, and is now actively implementing the criminal enforcement components of, the government-wide Joint Strategic Plan on Intellectual Property Enforcement unveiled in June 2010. We also actively participate in a number of IPEC-led working groups, including the counterfeit pharmaceutical interagency committee. As a result of that group's work, in March 2011 the IPEC transmitted to Congress the "Counterfeit Pharmaceutical Inter-Agency Working Group Report to the Vice President of the United States and to Congress." That report outlined government-wide efforts and a strategy to address this problem, including the IPEC-led effort to tackle the proliferation of illegal Internet pharmacies through voluntary cooperation in the private sector.

The Department has also worked on a series of legislative recommendations aimed at improving intellectual property enforcement. Those recommendations were included in the IPEC's government-wide "Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations" transmitted to Congress in March of this year. These recommendations include proposals for enhanced criminal penalties for intellectual property crimes, including economic espionage and trade secret theft. The White Paper also recommends enhancements to the criminal provisions of the Federal Food Drug and Cosmetic Act, reflecting the Department's efforts to prosecute aggressively counterfeit drug traffickers. These online drug dealers often make as much or more money than traditional narcotics traffickers and can reach far more consumers. Many escape serious penalties because they do not peddle narcotics or even controlled substances, but the threat to public health is no less severe. The White Paper also recommends creating a felony offense for illegally streaming pirated works, to reflect the increasing trend and threat from this type of widespread infringing conduct. And, the White Paper further seeks to give law enforcement the authority to seek wiretaps in criminal copyright and trademark cases – an important tool in our efforts to combat intellectual property crime, particularly to investigate organized criminal enterprises engaged in intellectual property crime.

I know that Congress has already begun to review many of these proposals and the Department very much appreciates Congress' consideration.

### **III. Role of the Department of Justice**

Intellectual property investigations and prosecutions can be complex, long-term, and increasingly involve sophisticated technology and technical efforts to locate and collect electronic evidence. To handle this complex and evolving area of enforcement, the Department has created a cadre of prosecutors and investigators who specialize in prosecuting computer and intellectual property crimes using particularized strategies and tools.

#### **A. CCIPS and the CHIP Program**

The Department implements its overall intellectual property criminal prosecution mission through its U.S. Attorney's Offices and CCIPS, including a network of over 260 specially-trained federal prosecutors who make up the Department's Computer Hacking and Intellectual Property (CHIP) Program.

CCIPS is a section within the Criminal Division consisting of a specialized team of 40 prosecutors who are devoted to the enforcement of computer crime and intellectual property laws. Fourteen CCIPS attorneys are assigned exclusively to intellectual property enforcement. These attorneys are the Department's core experts on intellectual property enforcement and are responsible for assisting in developing and implementing the Department's overall intellectual property enforcement strategy and legislative priorities. They also prosecute some of the most cutting edge and complex cases that are often multinational in dimension; they provide litigation support and training to assist prosecutors and investigators in the field; they provide training and capacity building internationally; and they ensure that federal prosecutors are apprised of all developments in intellectual property law that impact criminal enforcement.

For example, CCIPS attorneys have helped to apprise federal prosecutors across the country of the legal tools contained in Title II of the PRO IP Act. These include enhanced penalties for counterfeit goods that endanger public health and safety. The Act also clarified and harmonized forfeiture laws pertaining to intellectual property offenses, ensuring that civil and criminal forfeiture are available for all copyright, trademark, and theft of trade secret offenses, and that such forfeiture includes not only contraband, but also criminal proceeds and any facilitating property involved in the offense, including domain names. The Department has aggressively used this forfeiture authority to prevent defendants from keeping their ill-gotten gains and to deprive them of facilitating property essential to the commission of certain offenses, such as the domain names for websites that illegally distribute pirated and counterfeit goods.

The Department's national CHIP program now consists of a network of approximately 260 experienced federal prosecutors -- including Assistant U.S. Attorneys and attorneys in various sections and divisions at Main Justice -- who receive special training and ongoing support to aggressively pursue computer crime and intellectual property offenses. CHIP attorneys have four major areas of responsibility: (1) prosecuting computer crime and intellectual property offenses; (2) serving as the district's or office's legal counsel on matters relating to those offenses and to the collection of electronic or digital evidence; (3) training prosecutors and law enforcement personnel in the region; and (4) conducting public and industry outreach and awareness activities.

Each of the 94 U.S. Attorney's Offices has at least one CHIP coordinator. In addition, 25 U.S. Attorney's Offices have CHIP Units, with between two and eight CHIP attorneys. In December 2009, Congress provided funding under the PRO IP Act to support 15 positions in

CHIP Units around the country. The Department, through the Office of the Deputy Attorney General, Executive Office for U.S. Attorneys and the Criminal Division, identified the following districts with existing CHIP Units to support the new positions: California (two each in the Northern and Central Districts); the District of Columbia; Maryland; Massachusetts; the Eastern District of Michigan; New Jersey; New York (one each in the Eastern and Southern Districts); Pennsylvania; the Southern District of Texas; the Eastern District of Virginia; and the Western District of Washington. Those prosecutors are now all in place and, if the Department can continue to fund the positions over time, we anticipate that they will provide a tremendous boost to the Department's efforts to combat intellectual property crime.

#### **B. Law Enforcement**

Congress provided funding in FY 2009 and FY 2010 as authorized under the PRO IP Act that facilitated the hiring or assignment of 51 FBI special agents dedicated solely to investigating intellectual property crime and that supported training on investigating intellectual property crimes. My colleague here today from the FBI will no doubt address the Committee in more detail about these new agents; however, I can assure the Committee that these agents, the last of whom were placed at the end of 2010, have already enhanced the Department's ability to successfully prosecute intellectual property cases and will continue to do so in the future.

Through CCIPS, the Department also has provided extensive and ongoing support to the IPR Center. Under the capable leadership of its current Director, Bob Rutt, a strong foundation for future success has been built to combat counterfeiting and piracy, and the number of partners that have joined the Center has grown considerably to 15 federal regulatory and investigative agencies, and three international partners. I know my colleague from ICE will discuss the IPR Center in much greater detail.

#### **IV. Federal Enforcement Efforts**

The Department has sought to focus its investigative and prosecution efforts in areas involving some of the most egregious intellectual property offenses and in ways that will have the greatest impact on deterring intellectual property crime. Through the IP Task Force, the Department has identified as enforcement priorities those cases involving health and safety, trade secret theft and economic espionage, links to organized criminal enterprises, and large-scale commercial counterfeiting and piracy -- particularly those offenses occurring over the Internet. Already in 2011, we have prosecuted significant cases in each of our key enforcement areas, a few of which I would like to highlight briefly:

#### A. Health and Safety

- Just last month, as a result of an FDA criminal investigation, a defendant was indicted in the Eastern District of Pennsylvania for a scheme to sell approximately 6,000 boxes of counterfeit LifeScan One Touch diabetic test strips that he purchased from suppliers in China and England. The defendant sold wholesale quantities to customers in the United States and Canada, who, in turn, sold those counterfeit products to purchasers in pharmacies and other stores throughout the United States. This is particularly troubling given the serious nature of diabetes and potentially grievous effects of taking incorrect or ineffectual medication.
- Also last month, in the Eastern District of Virginia, two defendants were convicted on 16 separate counts by a federal jury for their roles in a sophisticated scheme to import and sell counterfeit Cisco computer networking equipment imported from China. The defendants conspired with family members in China who operated a large-scale counterfeit computer networking business. The jury also found that the defendants should forfeit seven bank accounts containing \$1.6 million in illegal proceeds, several luxury cars, and four homes and three condominiums worth more than \$2.6 million. Notably, this case began with a criminal referral by U.S. Customs and Border Protection (CBP), and was investigated by ICE as well as the Offices of the Inspector General for both the General Services Administration and the U.S. Department of the Interior.
  - The aforementioned prosecution builds upon *Operation Network Raider*, a major international law enforcement initiative that targeted the illegal distribution of counterfeit network hardware manufactured in China. When the Department of Justice, ICE, CBP, and the FBI announced the operation last year, it had already resulted in 30 felony convictions and more than 700 seizures of counterfeit Cisco network hardware and labels with an estimated retail value of more than \$143 million. Through aggressive investigation and prosecution, the operation seeks to protect computer networks and the nation's IT infrastructure from failures associated with counterfeit network hardware, including network routers, switches, network cards, and devices that protect firewalls and secure communications that have been intercepted both domestically and abroad.
- In February 2011, in the Eastern District of Michigan, a defendant was sentenced to 46 months in prison on multiple charges relating to his role in illegally importing and selling thousands of doses of counterfeit and misbranded drugs. Again, this case resulted from a multi-agency effort, combining the investigative efforts of ICE, CBP, the U.S. Postal Inspection Service, and the FDA.

**B. Trade Secret Theft and Economic Espionage**

- In April 2011, also in the Eastern District of Michigan, a former Ford Motor Company product engineer was sentenced to 70 months in prison for misappropriating thousands of pages of sensitive and valuable resource and design information specifications from Ford, reflecting millions of dollars in research and development. The FBI investigation determined that he used the design information to benefit the Beijing Automotive Company, a Chinese direct competitor of Ford. The defendant stole the trade secret information before disclosing to Ford that he was leaving the company.
- In March 2011, in the Southern District of New York, a former computer programmer at the investment bank Goldman Sachs was sentenced to 97 months in prison for misappropriating proprietary computer code worth \$500 million that was used for high-frequency securities trading.
- In February 2011, a federal jury in Baton Rouge, Louisiana, convicted a former Dow Chemical Company research scientist of conspiracy to commit trade secret theft and perjury. The defendant, who had worked for Dow for 30 years, had misappropriated valuable trade secrets concerning the development and manufacture of certain chemicals. He sold these trade secrets to Chinese companies in an effort to develop and market competing technologies in China. Like the previous case, this was the result of an FBI investigation.

**C. Organized Criminal Enterprises**

- In May 2011, a defendant pleaded guilty in the Central District of California to charges arising from his role in operating an online music release group called “Old School Classics” (OSC). The FBI investigation revealed that OSC is a “warez” group that specialized in the unauthorized reproduction and distribution of copyrighted music over the Internet. Warez groups are organized enterprises that operate as first-providers of copyrighted works. These groups obtain copyrighted works, sometimes from industry insiders before the work’s commercial release, and then prepare the works for distribution. Once a warez release group prepares a stolen work for distribution, the material is distributed to servers of affiliated warez groups and ultimately worldwide through peer-to-peer networks.
- In January 2011, two defendants were sentenced in the Eastern District of Virginia to 18 and 10 months in prison, respectively, for conspiring to traffic in, trafficking in, and illegally smuggling counterfeit luxury goods imported from China. The ICE investigation determined that the defendants controlled a massive international counterfeit goods business through which they imported over

300,000 counterfeit luxury handbags and wallets into the United States from China with an estimated retail value of over \$100 million. The defendants operated at least 13 shell companies and 8 manufacturing plants in China.

**D. Large-Scale Commercial Counterfeiting and Online Piracy**

- The Department has made use of the forfeiture authorities I described earlier in a joint initiative with ICE known as *Operation In Our Sites*. This ongoing initiative seeks to seize domain names associated with websites that distribute pirated and counterfeit goods. The owners of these websites are usually located overseas and therefore are unlikely ever to be brought to the U.S. to face charges. There have been a number of such seizures, including as recently as last month. Perhaps the largest and most significant number of seizures occurred in November 2010, on “Cyber Monday,” just after Thanksgiving -- known as the busiest online shopping day of the year. On that day, the Attorney General and ICE Director John Morton announced the results of *Operation in Our Sites v.2.0*, which resulted in the seizure of over 80 Internet domain names of domestic and international businesses selling a diverse array of counterfeit and pirated goods. The operation disrupted the sale of thousands of infringing items, cut off funds to those seeking to profit illegally from the hard work of others, and served to remind consumers to exercise caution when looking for deals and discounts online.
- In May 2011, a husband and wife were each sentenced in the Central District of California to 37 months in prison, while a co-conspirator received 30 months’ imprisonment, for their respective roles in importing and selling to merchants in at least five states thousands of counterfeit pieces of designer jewelry with an estimated retail value of over \$18 million. The ICE investigation determined that all of the counterfeit jewelry was manufactured in China. Lab tests revealed that some of the counterfeit products contained nearly 20 times the amount of lead deemed safe by the Consumer Product Safety Commission for handling by children.
- In January 2011, a federal judge in New Jersey sentenced Michael Hanna to 60 months imprisonment for his convictions for conspiracy to bribe public officials and to import counterfeit luxury goods. He admitted that between June 2008 and March 2009 he paid more than \$700,000 in cash to a person he believed to be acting at the direction of a corrupt U.S. Customs and Border Protection official. Hanna made the cash payments in an effort to ensure that at least fifteen containers of counterfeit merchandise ranging from sneakers, handbags, pocketbooks, and other items were not detained or seized at a port of entry.

#### IV. Outreach and Support to State and Local Law Enforcement

The Department realizes that federal law enforcement is not the only answer to reducing intellectual property crime. To maximize our effect in addressing all forms of intellectual property crime, the IP Task Force has prioritized enhancing coordination with state and local law enforcement.

The Department's efforts to leverage the skills and capacity of state and local law enforcement are also consistent with the goals of § 401 of the PRO IP Act to create a grant program available for state or local law enforcement entities for the purpose of "training, prevention, enforcement, and prosecution of intellectual property theft and infringement crimes" (known as IP-TIC grants). The Office of Justice Programs (OJP), through its Bureau of Justice Assistance (BJA), has, using discretionary funding, offered competitive grants during all three fiscal years since enactment of the PRO IP Act. These grants have been used to support local IP task forces and local IP training and technical assistance.<sup>1</sup> In FY 2009 and FY 2010, OJP made 27 awards totaling approximately \$6.5 million to 18 state and local criminal justice agencies and three non-profit law enforcement member organizations (nine of them were two-time recipients). The competitive grant process for FY 2011, for which OJP anticipates awarding "multiple grants of up to \$200,000," ended on February 10, 2011.

These OJP grant programs are designed to provide national support and improve the capacity of state and local criminal justice systems to address criminal intellectual property enforcement, including prosecution, prevention, training, and technical assistance. The programs also encourage grant recipients to coordinate their efforts through multi-jurisdictional task forces, and appropriate federal agencies, including the local FBI and U.S. Attorney's Offices.

These grants have been the foundation for numerous successful investigations during the past year. A few examples of these successes include:

- The San Antonio Police Department made arrests in February at two stores that were selling counterfeit merchandise. Law enforcement seized 1,780 pieces of counterfeit merchandise and cash proceeds, with a total estimated value of \$129,612.61;
- Last January, based on undercover purchases, the Los Angeles Police Department's Anti-Piracy Unit arrested a defendant for selling counterfeit Sony cameras. The LAPD seized over \$40,000 in cash proceeds and \$10,000 in cashier's checks and money orders. Detectives also determined that the defendant supplied counterfeit cameras to multiple area vendors and was connected to other targets arrested for intellectual property crimes that had occurred in the City of Industry and San Diego, California;

---

<sup>1</sup> The grant program has operated under slightly different titles: FY 2009, the "Intellectual Property Enforcement, Training, and Technical Assistance Program;" in FY 2010, the "Intellectual Property Enforcement Program;" and in FY 2011, the "Intellectual Property Crime Enforcement Program."



- Working closely with the FBI and ICE, the Sacramento Valley Hi-Tech Crimes Task Force investigated and dismantled a significant counterfeiting operation in San Jose, California that was responsible for trafficking in significant quantities of pirated music and movies throughout Central and Northern California. As a result, in November 2010, they seized approximately \$2 million in counterfeit CDs and DVDs as part of this operation and grand jury in Fresno, California returned an indictment charging eight individuals with conspiracy to commit criminal copyright infringement and trafficking in counterfeit labels in January 2011; and
- Based on a referral by the Recording Industry Association of America in August 2010, the Chesterfield County Police Department in Chesterfield, Virginia conducted a several-month investigation into the sale of counterfeit CDs and DVDs at a local flea market. Based on that investigation, in October 2010, a Multi-jurisdiction Special Operations Group (MSOG) task force executed nine search warrants at the flea market, arresting 11 individuals and seizing 30,098 counterfeit CDs and DVDs containing pirated music with an estimated retail value of \$200,000, along with \$1,145 in cash. The MSOG task force included the Chesterfield County Police Department, the City of Richmond Police Department, and Virginia State Police.

Beyond OJP's grant programs, the Department looks for other opportunities to encourage state and local law enforcement collaboration on intellectual property investigations and prosecutions. For example, CCIPS has organized and led approximately 10 conferences in the past four years which brought together right holders and federal, state, and local prosecutors. These one-day instructional seminars provided state and local law enforcement with an opportunity to discuss aspects of intellectual property crime with federal law enforcement experts as well as businesses, private investigators, and corporate counsel. In the last year, the Department has also participated in intellectual property training seminars for state and local law enforcement sponsored by the IPR Center in Philadelphia, Denver, San Juan, San Jose, San Diego, Detroit, San Antonio, Minneapolis, and Portland.

#### **V. International Enforcement Efforts**

To be sure, combating intellectual property crime effectively requires strong domestic enforcement efforts, but that is only one part of a much broader strategy. To be truly effective, our response to intellectual property crime must be global in nature. We must look beyond our borders to develop a forceful and effective international enforcement program. The Department's international enforcement efforts are multi-faceted, including prosecutions, training, and capacity building. Moreover, Department prosecutors participate in strategic bilateral and multi-lateral criminal enforcement working groups with a number of countries that we deem important to effective global enforcement. These efforts are designed (1) to increase international intellectual property prosecutions that disrupt foreign manufacturers and trans-border shipments of pirated and counterfeit products, and (2) to dismantle international organized

criminal syndicates engaged in intellectual property crimes. Notably, the PRO IP Act's call for the formulation of an organized crime plan dovetails with the Department's long-standing commitment to fighting organized crime and its more recent efforts to confront the shift of organized crime syndicates from more traditional crimes like drug trafficking to intellectual property crimes.

#### **A. International Outreach and Training**

The Department works with other countries to develop effective criminal intellectual property enforcement regimes. Ensuring that all countries are equipped and motivated to enforce criminal intellectual property laws is critical to reducing safe havens for intellectual property criminals. The Department's outreach and training efforts on intellectual property are accomplished by direct work on specific cases; through targeted training and capacity-building programs coordinated by the Criminal Division's Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) and CCIPS, frequently in coordination with the State Department and other U.S. agencies – most notably DHS (ICE and CBP) and the USPTO; through leadership of bilateral groups such as the Intellectual Property Criminal Enforcement Working Group (IPCEWG) of the U.S.-China Joint Liaison Group for Law Enforcement Cooperation; and multi-lateral bodies such as Asia-Pacific Economic Cooperation (APEC) and the Department-led IP Crimes Enforcement Network (IPCEN) in Asia; and with international law enforcement groups such as the World Customs Organization and INTERPOL.

##### **1. Training**

In 2010 alone, the Department trained or educated over 2,500 foreign judges, prosecutors, investigators and other international intellectual property officials in over 33 countries on intellectual property protection. This is in addition to over 10,000 officials receiving such training or education in the prior five years. The Department is also providing more targeted training. For example, recent efforts have included computer forensic training seminars for a number of IPCEN nations in Asia; IP enforcement training programs in Mexico focusing on intellectual property crime at the border; judicial training on adjudicating cases involving intellectual property crimes for seven southern African nations in Rwanda; and counterfeit pharmaceutical training programs for customs officials in Mexico and sub-Saharan Africa.

The Department also provides criminal enforcement experts to support intellectual property training programs sponsored by other agencies. Just this year, the Department provided substantial assistance to programs hosted by USPTO and the IPR Center in Pakistan, Hong Kong, El Salvador, Lithuania and Ukraine.

## **2. Asia/China**

The Department's commitment to international cooperation comes from the top. In October 2010, the Attorney General delivered the keynote address at the Fourth Annual International Law Enforcement Intellectual Property Crime Conference in Hong Kong, which was hosted by INTERPOL and Hong Kong Customs in partnership with Underwriters Laboratory. In attendance were more than 500 law enforcement agents, prosecutors, and industry representatives from approximately 40 countries. As the Attorney General recognized in his remarks, "[t]ogether, we are signaling that a new era of cooperation, engagement, and vigilance has begun. And we are sending an unequivocal message to criminals profiting from the ingenuity of others or endangering the safety of our citizens by selling defective or dangerous counterfeit goods. We will find you. We will stop you. And you will be punished."

Although no one country stands alone as the cause of global intellectual property crime, China is a significant source of counterfeit and pirated products imported into the United States as well as trade secret theft. For this and other reasons, following his trip to Hong Kong, the Attorney General traveled to Beijing, China, where he attended meetings with China's Minister of Public Security, the Chief Procurator and Politburo Member responsible for law enforcement, among others. The Attorney General emphasized the importance of intellectual property enforcement and secured commitments from China both to enhance its domestic enforcement of intellectual property rights and to improve its cooperation on transnational intellectual property crime investigations. Coinciding with the Attorney General's meeting, China's State Council announced a six-month crackdown on counterfeit and pirated goods, known as the Special Campaign. By most accounts, the Special Campaign, which has been extended through this month, has resulted in increased domestic enforcement as well as greater coordination among intellectual property authorities in China and has led to increased domestic enforcement in certain areas. At the U.S.-China Strategic and Economic Dialogue in early May, China pledged to improve its long-term intellectual property enforcement efforts drawing on the lessons of the Special Campaign.

## **3. IP Law Enforcement Coordinator Program**

Another key component of the Department's international enforcement efforts has been the Department's IP Law Enforcement Coordinator (IPLC) program, first established in 2006, through a partnership between a partnership between OPDAT and CCIPS. The Department has had two experienced prosecutors posted in Bangkok, Thailand and, until recently, in Sofia, Bulgaria, covering Asia and Eastern Europe, respectively. Unfortunately, we were not able to continue the Eastern Europe position once State Department funding for the position ran out in March of this year. We do, however, appreciate the State Department's support for the program over the last three-plus years.

However, because the IPLEC program has a strong and proven track record of success, President Obama asked Congress in his 2012 budget request to fund a new Department program that would place six International Computer Hacking and Intellectual Property coordinators, or “ICHIPs,” in key locations around the world. The ICHIP program would build on and expand the IPLEC program to strengthen our international intellectual property efforts as well as to support the Department’s international organized crime strategy as it relates to intellectual property, online fraud, and large-scale data breaches that threaten U.S. economic security in targeted regions worldwide.

## **B. Organized Crime Networks**

In enacting the PRO IP Act, Congress recognized a growing concern that organized criminal enterprises have begun to engage in intellectual property crime. It is not surprising that organized crime groups have turned to the sale of counterfeit and pirated goods as a revenue source given the perception that intellectual property crime is a low-risk criminal enterprise with the potential for high profit margins. This is a serious concern, particularly in Asia, but also in other parts of the world, including countries in the former Soviet Union and the Tri-border region of South America. Organized crime syndicates have the ability and the resources to manufacture and move massive amounts of counterfeit products around the globe.

In § 402(b) of the PRO IP Act, Congress directed the Attorney General, subject to the availability of appropriations, to create and implement a comprehensive, long-range plan to investigate and prosecute international organized crime syndicates engaging in or supporting IP-related crimes. Although Congress has not yet appropriated any funds to support this provision, the Department, consistent with its long-term commitment to fighting organized crime in all forms, has taken several steps to implement the goals of § 402(b) and to make intellectual property crimes an integral part of its overall organized crime strategy.

As I indicated at the outset of my remarks, the Department’s IP Task Force has designated the prosecution of crimes perpetrated by organized crime syndicates as a priority in its intellectual property enforcement efforts. Likewise, direction from senior Department leadership has resulted in a range of activities designed to increase information sharing between the Department’s organized crime prosecutors and investigators and those focused on intellectual property crime. It has also generated numerous training programs and events designed to educate law enforcement and regulatory officials about the growing links between organized crime and intellectual property crimes. Similarly, the Attorney General’s Organized Crime Council (AGOCC)<sup>2</sup> has prioritized intellectual property enforcement, adopting as part of its 2010 Action

---

<sup>2</sup> The AGOCC comprises the Deputy Attorney General (Chair), the Assistant Attorney General, Criminal Division, the Chair of the Attorney General’s Advisory Committee; and the heads of the following nine participating law enforcement agencies: FBI; Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms and Explosives; ICE-HSI; U.S. Secret Service; Internal Revenue Service; Criminal Investigation; U.S. Postal Inspection Service; U.S. Department of State; Bureau of Diplomatic Security; and the U.S. Department of Labor, Office of the Inspector General.

Plan a specific goal to enhance law enforcement coordination in this important area.

Under the guidance of the IP Task Force and the AGOCC, and in the absence of additional appropriations, the Department has focused on two primary goals: (i) increasing information sharing and coordination between the federal entities responsible for investigating and prosecuting organized crime and intellectual property crimes; and (ii) providing training and outreach for Department prosecutors and federal agents, and also for our foreign law enforcement partners, on the growing links between organized crime and intellectual property crimes.

In order to increase information-sharing and coordination between organized crime and intellectual property crime prosecutors and investigators, the Department has taken the following measures:

- Just, two weeks ago, on June 10, the Assistant Attorney General Lanny Breuer announced a new position in the Criminal Division to recognize the high priority placed on transnational organized crime issues -- Counselor for Transnational Organized Crime and International Affairs. This position will be filled by Bruce Ohr, one of our most senior prosecutors and experts in this area. He will play a critical role in leading and coordinating the Department's work in this area which will include our continued efforts to identify and address the links between organized crime and intellectual property crime;
- CCIPS has detailed a senior attorney to the International Organized Crime Intelligence and Operations Center ("IOC-2"), who now serves as the Acting Director, reporting to the AGOCC;
- All relevant agencies with a stake in criminal intellectual property investigations are contributing intellectual property data to IOC-2, including the FBI, ICE-HSI and CBP;
- IOC-2 is working with the IPR Center to develop protocols to cross-train personnel at the two centers and to govern their respective efforts to identify those intellectual property violations that involve organized crime; and
- OCRS and CCIPS regularly conduct case reviews to determine whether further coordination is appropriate.

Just this year, the Department has undertaken the following training and outreach measures to educate both domestic law enforcement and our foreign partners on the importance of searching for links between organized crime and intellectual property crimes:

- In May 2011, CCIPS provided training on the collection and analysis of electronic evidence, with special emphasis on intellectual property crimes, to organized crime prosecutors and law enforcement officers in Mexico, and a follow-up training session is planned;
- In March 2011, at the Department's annual five-day CHIP Conference, which brought together nearly 200 CHIP prosecutors from USAOs across the country, IOC-2 gave a briefing on the tools it offers to prosecutors and federal agents investigating cases which involve both organized crime and intellectual property crimes; and
- Also in March 2011, at the APEC Dialogue on Corruption and Illicit Trade, CCIPS organized and moderated a panel discussion on best practices for combating the widespread and trans-global trade in counterfeit medicines, increasingly the domain of organized crime syndicates, featuring law enforcement and regulatory officials from Europe, Latin America, and the Far East.

### **Conclusion**

We have accomplished a great deal and made significant strides in combating intellectual property crime both here and abroad. But as we all know, there is much more that needs to be done. The Attorney General is personally committed to ensuring that the Department's enforcement efforts continue to stay one step ahead of intellectual property criminals. We will continue to make efficient use of our resources to bring them to justice, to protect the health and safety of the American people, and to safeguard one of this country's greatest assets.

This concludes my remarks. I would be pleased to answer questions from you and other members of the Committee.

PREPARED STATEMENT OF GORDON M. SNOW, ASSISTANT DIRECTOR, CYBER DIVISION,  
FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, DC



## **Department of Justice**

---

STATEMENT OF

GORDON M. SNOW  
ASSISTANT DIRECTOR  
CYBER DIVISION  
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON JUDICIARY  
UNITED STATES SENATE

ENTITLED

"Oversight of Intellectual Property Law Enforcement Efforts"

PRESENTED

June 22, 2011

Good afternoon Chairman Leahy, Ranking Member Grassley, and members of the Committee. I'm pleased to appear before you today to discuss the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO IP Act) and the FBI's efforts, activities, and successes relating to intellectual property rights (IPR) crimes to date.

The enforcement of U.S. laws protecting IPR is critical to protecting the U.S. economy, our national security, and the health and safety of American citizens.

The increasing accessibility of the Internet and improvements in manufacturing and transportation have led to the expansion of the global market. With increasing competition, innovation, and divisions of labor, more digital content is instantaneously distributed to the global market than ever before. Businesses now have extraordinary opportunities to market and distribute their goods and services all around the world.

Unfortunately, the expansion in worldwide trade has led to growth in the number of criminals and organizations that seek to exploit and misappropriate the intellectual property of others for profit. These criminals have developed complex and diverse methods of committing IPR crime.

#### **The Nature of the Threat**

IPR violations which include theft of trade secrets, digital piracy, and the trafficking of counterfeit goods, result in billions of dollars in lost profits annually. Failure to protect IPR undermines confidence in the economy, removes opportunities for growth, erodes the U.S.'s technological advantage, and disrupts fairness and competitiveness in the marketplace. In short, a robust system for protecting IPR is critical to economic prosperity.

However, some IPR violations pose a more far-reaching and serious threat to the U.S. than just economic loss to the rights holder. Such violations put public safety at risk through the sale of counterfeit pharmaceuticals, electrical components, aircraft and automobile parts, and the funding of organized crime.

Some IPR violations also threaten our critical infrastructures and our national security. Counterfeit computer and networking devices undermine the reliability of our communications and transportation networks and create national security vulnerabilities. In addition, nation states target U.S. civilian industries for trade secret theft to obtain information that can be used to advance domestic industries and military capabilities.

The focus of my remarks today is the important role the FBI plays in protecting IPR, our efforts to coordinate with other federal agencies to ensure that intellectual property is rigorously protected, and our successes in this battle thus far.



### **The Role of the FBI**

The FBI's strategic objective is to detect and disrupt state sponsored groups and international and domestic criminal organizations that manufacture counterfeit and pirated goods or steal, distribute or otherwise profit from the theft of intellectual property. The highest priorities for our investigations are counterfeit products affecting health and safety, the theft of trade secrets, and violations with a significant economic impact. The FBI aggressively pursues intellectual property enforcement through traditional investigative methods, intelligence initiatives and coordinated efforts with private industry and domestic and foreign law enforcement partners.

The FBI partners closely with the National Intellectual Property Rights Coordination Center (the IPR Center), which is hosted by U.S. Immigration and Customs Enforcement (ICE). The IPR Center serves as a centralized, multiagency entity to coordinate, manage, and advocate the U.S. government's criminal enforcement of intellectual property laws.

The FBI moved its Intellectual Property Rights Unit (IPRU) to the IPR Center in April 2010. It includes five dedicated FBI agents, as well as management staff, intelligence analysts and professional support staff who work full time at the IPR Center. The IPRU has a dual focused mission. First, it provides effective national program management for the FBI IPR program by aggressively advocating program awareness, coordinating and deconflicting investigative activity, and proactively developing relationships to address current and emerging threats to U.S. intellectual property. Second, it initiates and conducts IPR investigations that are complex, multi-jurisdictional and/or international in nature.

The IPRU is the coordination center for field office efforts to investigate IPR violations and other FBI divisions that conduct investigations with an IPR nexus. For example, the Criminal Investigative Division's Organized Crime Unit investigates cases involving counterfeit health products. The Counterintelligence Division's Economic Espionage Program focuses on the theft of trade secrets by foreign agents, governments and instrumentalities as defined by the Economic Espionage Act of 1996. Collaboration with these two divisions on IPR cases functions as a force multiplier and leads to broader criminal charges and higher penalties for offenders.

### **The FBI and the PRO IP Act**

As a result of the PRO IP Act, the FBI Cyber Division has 51 dedicated IPR special agents placed in 21 field offices and the IPRU. The first enhancement under the Act, in April 2009, resulted in the allocation of 26 positions in the field and five at the IPRU. A second enhancement in May 2010 led to the allocation of an additional 20 positions in the field. Of these 51 positions, 44 special agents were placed in 20 field offices where United States Attorneys' Office (USAO) had Computer Hacking and Intellectual

Property (CHIP) Units. The FBI office in Houston was allocated two IPR agents, even though there is not a CHIP unit there, for a total of 46 agents in the field.

As part of this allocation, the field offices in Los Angeles, New York, San Francisco, and Washington, D.C. received an enhancement to establish dedicated IPR squads. Each of these offices has established IPR task forces or working groups to coordinate IPR enforcement efforts and conduct outreach to industry and rights holders.

This distribution of investigative resources maximizes the nationwide reach and ability of the FBI to disrupt and dismantle international and domestic manufacturers or distributors of counterfeit and pirated goods, and criminal organizations engaged in IPR crime. The locations for the distribution of these resources were selected based on a regional domain analysis of the threat to intellectual property, intellectual property threat intelligence reporting, input from the IPR Center, and an understanding that the geographically-dispersed nature of IPR violations and subject locations made it possible to establish venues regionally. The placement of the special agents was coordinated with and approved by the Office of the Deputy Attorney General and the Executive Office of the United States Attorneys.

As of May 31, 2011, the FBI had 471 pending IPR investigations with 46 special agent positions dedicated to working IPR matters in the field. In FY 2010, the number of new FBI initiated theft of trade secrets and health and safety cases increased by 42 percent over FY 2009. The use of sophisticated investigative techniques increased by 50 percent in IPR cases.

In addition to the placement of IPR dedicated agent resources, in the spring of 2010, the IPRU management team conducted a case review of all pending IPR cases to support the shift of resources to priority investigations.

### **Strategic Initiatives and Successes**

Capitalizing on the resources from the PRO IP Act, the FBI has enhanced its engagement on a number of significant strategic initiatives. This engagement has sharpened the focus of the FBI's IPR program on priority threats, increased awareness of the threat landscape, and strengthened relationships with community partners.

The FBI established and leads the Intelligence Fusion Group (IFG) at the IPR Center. Together the partner agencies define the IPR threat picture, share tactical and strategic intelligence, produce joint intelligence products, and develop the national strategy to address IPR crimes. Through the IFG, the FBI led a comprehensive analysis of the global threat to U.S. interests from criminal IPR violations. The report, entitled "Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad," is the culmination of a year-long joint effort led by the FBI and ICE with contributions from IPR Center partners. As part of this effort, agents and analysts interviewed 126 IPR experts from corporate security offices, industry associations, government agencies, and academic institutions in the U.S., India, and China regarding

IPR threats. A survey accompanying the report will solicit feedback and additional information to help determine additional targeted analysis opportunities.

To address the problem of counterfeit aircraft parts entering the commercial and military repair or manufacturing supply chain, the FBI, Department of Transportation Office of Inspector General and Federal Aviation Administration jointly coordinated the “Fractured Skies” initiative. As part of this effort, the IPRU has engaged the National Cyber-Forensics & Training Alliance, located in Pittsburgh, PA, for analytical review and target package development.

In an effort to improve international relationships on IPR investigations, conduct threat assessments, and make recommendations on the strategic plan in high threat countries, the IPRU embedded a dedicated IPR team comprised of an analyst and an agent in the FBI’s Legal Attaché offices in Beijing and New Delhi to work directly with local and regional authorities on IPR matters for 60 days. Based upon the results of this effort and the threat emanating from these regions, the IPRU is currently in the process of embedding a fulltime IPR dedicated agent in Beijing for a year.

To capitalize on private sector partnerships, the FBI created a working group consisting of corporate security officers from Fortune 100 companies to focus on bolstering relationships of trust between law enforcement agencies and industry and improving information-sharing regarding intellectual property theft. In February 2011, the FBI hosted key industry Chief Security Officers to kick-off the Intellectual Property Threat Small Working Group. The goal of this working group is to build liaison among industry peers in an effort to generate high priority IPR cases. To this end, the FBI is currently developing targeted education and awareness presentations for corporate executives and general counsels.

Additionally, the FBI has taken over the hosting of the IPR Center’s website, [www.IPRCenter.gov](http://www.IPRCenter.gov). Phase two of this project will kick off later this year and involved a significant redesign of the site so that it includes training, education, enforcement activities and a reporting mechanism for IPR tips. The FBI is working in concert with the IPR Center partners to ensure comprehensive coverage of IPR issues and make this site the “go to” site for all IPR enforcement.

### **Training and Capacity Building**

In order to promote high standards of IPR protection and the enforcement of laws protecting intellectual property, the FBI places a heavy emphasis on meaningful training and capacity building. The FBI provides training on IPR enforcement to an increasing number of individuals each year. In FY 2009, the FBI provided IPR training to 782 individuals from the federal government, the domestic private sector, foreign governments, and the overseas private sector. In FY 2010, the FBI trained 1678 such individuals. As of May 2011, the FBI has already trained 1064 individuals. As described below, the FBI provides training to its own personnel and its domestic and international

counterparts in a number of different ways. Resources from the PRO IP Act have made these ambitious and important training programs possible.

In September 2010 the IPRU provided its second annual, comprehensive IPR program training for IPR dedicated special agents. Additionally, special agents new to the IPR program received an introductory basic training course, and all IPR special agents participated in an advanced course to build upon existing skill sets and share the latest investigative techniques and technological methods.

IPR program coordinators in offices currently without funded IPR positions also received this annual training to ensure maximum regional coverage and to provide support to the CHIP units. The training session explored the forensic aspects of IPR investigations, to include the mechanisms necessary to identify counterfeits, the utilization of undercover operations, and IPR evidentiary procedures. Training topics also covered statutory authorities, DOJ enforcement efforts, major case initiatives, case studies, intelligence analysis for IPR cases, and federal partnering efforts. Industry subject matter experts from the International Anti-Counterfeiting Coalition, Underwriters Laboratories, Eli Lilly, Cisco Systems, the Motion Picture Association of America, and Microsoft made presentations.

All cyber career path designated special agents receive supplemental IPR training during a two-week New Agent Training (NAT) program. This training consists of an IPR program overview, a PRO IP Act overview, IPR case initiation/investigative techniques, and guidance regarding the importance of interagency partnerships, and the benefits of industry coordination efforts. The agents also receive forensic training from the Computer Analysis Response Team (CART) of the Operational Technology Division at FBI.

The IPRU recently developed a comprehensive web based training module specifically designed for agents working on IPR investigations. This module will be placed on our online training academy in the very near future.

The FBI also provides cross-program IPR training to organized crime and counterintelligence special agents and training on organized crime and counterintelligence to IPR dedicated special agents. This cross-program training was designed to ensure that agents pursue all avenues of investigation in cases that involve organized crime, counterintelligence and IPR issues.

The FBI provides IPR training to domestic and international law enforcement officials. The FBI is collaborating with its partner agencies to develop more comprehensive and advanced intellectual property training curriculum. The curriculum will ensure a uniform foundation across law enforcement agencies conducting IPR investigations and provide state and local law enforcement and industry liaisons with information about how to most effectively partner with the federal government on IPR investigations. For example, the FBI contributed training material and support to INTERPOL's new Intellectual Property

Crime College, an online resource available to law enforcement officers and industry partners worldwide.

Over the last two years, the FBI, through the IPRU, provided training on IPR to law enforcement officials from 15 different countries. For example, in September 2010, the FBI provided training during the 6th INTERPOL and Korea Copyright Commission Conference in Seoul, South Korea. It was the first to be held in the INTERPOL Asia and Pacific Region and was delivered with the support of the INTERPOL Liaison Office Bangkok for Asia and Pacific Region. The target audience included regional police middle managers with responsibility for investigating transnational organized intellectual property crime. The training provided attendees with a common understanding of the nature and extent of regional and increasingly global transnational organized intellectual property crime and investigative best practices techniques. It illustrated the benefits of working together with industries affected by intellectual property crime.

Additionally, the FBI provided training to the U.S. Patent and Trademark Office and its international attachés. The FBI's use of PRO IP Act resources has permitted an increased focus on training in high priority areas; this has directly contributed to increases in the quantity and quality of IPR cases.

#### **Investigative Accomplishments**

Pro IP Act resources have directly contributed to the FBI's development of strategic initiatives, training of its agents and counterparts, and increased capacity to combat high priority IPR crime. As a result, over the past year, the FBI and its partners have successfully investigated major IPR violations that resulted in millions of dollars in losses and unquantifiable harm to human health and safety. The following are but a few examples.

Earlier this year, a former Apple employee pled guilty to his role in a scheme to defraud Apple, Inc. while he was employed with the company from 2005 through 2010. The FBI investigation began in April 2010, when Apple found evidence of a kickback scheme on the employee's laptop. The employee transmitted Apple's confidential information, such as product forecasts, roadmaps, pricing targets, product specifications, and data obtained from Apple's business partners, to suppliers and manufacturers of Apple parts. In return, the suppliers and manufacturers paid kickbacks, including payments determined as a percentage of the business they did with Apple. The scheme enabled the suppliers and manufacturers to, among other things, negotiate more favorable contracts with Apple than they would have been able to obtain without the confidential information.

A joint investigation with an FBI counterintelligence squad revealed that General Motors (GM) was allegedly the victim of a conspiracy by a former GM employee and spouse to steal GM's hybrid vehicle technology with the intent to sell it to a Chinese automaker. The stolen GM documents were valued at over \$40 million. The couple was arrested on July 22, 2010.

Last year, the FBI initiated a case involving the theft of trade secrets at Societe Generale (SocGen). On November 19, 2010, the former employee was found guilty of theft of trade secrets and interstate transportation of stolen property for stealing the proprietary computer code used in SocGen's high-frequency trading system; he was sentenced to three years in prison.

Similarly, a former employee of Goldman Sachs was convicted for theft of trade secrets in 2010. The defendant, a computer programmer, was accused of stealing trading software by uploading a proprietary trading platform program for equity products to a server in Germany. The FBI was able to seize the server in question and block access to the site. Goldman Sachs could not put an exact dollar amount on the software taken, but media reports have indicated that Goldman made in excess of \$300 million in one year through its use of high frequency program trading and would not license the software for anything less than \$1 billion. In December 2010, a federal jury found the defendant guilty of theft of trade secrets; in March 2011, he was sentenced to 97 months in prison.

Highlighting the potential for safety risks associated with some IPR violations, a Canadian man was sentenced to 33 months in prison for selling fake cancer medication on the Internet. Initial investigation into the sale and distribution of copyrighted media revealed that the subject was marketing fake cancer treatment drugs, which he admitted to selling to at least 65 cancer patients. In addition to his prison sentence, he was ordered to pay a \$75,000 fine and \$53,724 in restitution.

In January of this year, Wayne Chih-Wei Shu pled guilty to six counts of mail fraud, one count of trafficking in counterfeit goods, and one count of trafficking in counterfeit labels, illicit labels, or counterfeit documentation or packaging. The case was initially based on intelligence provided by Microsoft's Anti-piracy group which identified Shu as one of the most prolific distributors of counterfeit Microsoft server and Office software in Washington state. The investigation resulted in the seizure of the counterfeit evidence, as well as a forfeiture judgment for the sum of \$1,750,396.98, for real and personal property, cash, and illicit proceeds.

### **Conclusion**

As the Committee knows, law enforcement faces significant challenges in our efforts to protect IPR, thereby protecting U.S. IP right holders and the health and safety of American citizens.

With the support of the PRO IP Act, however, the FBI is in a position to aggressively investigate the domestic and international criminal organizations that profit from the theft of intellectual property. The PRO IP Act has enabled the FBI to dedicate increased numbers of special agents and analysts to IPR matters, ensure quality training, and support effective interagency collaboration. Combined with our ongoing efforts to strengthen our relationships with industry, partner with our counterparts in the IPR Center and improve our collaboration with our international law enforcement partners, these efforts will enhance our ability to identify and neutralize those who perpetrate IPR

crimes.

We look forward to working with the Committee and Congress as a whole to continue on a successful course forward for the nation that protects intellectual property and its citizens. Thank you for the opportunity to be here. I would be happy to take any questions.

PREPARED STATEMENT OF ALLEN GINA, ASSISTANT COMMISSIONER, OFFICE OF INTERNATIONAL TRADE, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC



## U.S. Customs and Border Protection

---

STATEMENT

OF

ALLEN GINA  
ASSISTANT COMMISSIONER  
OFFICE OF INTERNATIONAL TRADE

U.S. CUSTOMS AND BORDER PROTECTION  
DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

“OVERSIGHT OF INTELLECTUAL  
PROPERTY LAW ENFORCEMENT EFFORTS”

BEFORE THE

UNITED STATES SENATE  
COMMITTEE ON THE JUDICIARY

Wednesday, June 22, 2011 - 10:00 a.m.  
226 Dirksen Senate Office Building



**INTRODUCTION**

Chairman Leahy, Ranking Member Grassley, and distinguished Members of the Judiciary Committee, I am pleased to appear before you today alongside witnesses from several government agencies, including Assistant Deputy Director Erik Barnett from our Department of Homeland Security sister agency U.S. Immigration and Customs Enforcement (ICE), to discuss the actions we are taking at U.S. Customs and Border Protection (CBP) to ensure that the laws governing intellectual property rights (IPR) are properly enforced for goods imported to and exported from the United States.

My name is Allen Gina and I am the Assistant Commissioner for the Office of International Trade at CBP. My office is responsible for formulating CBP's policies on commercial trade, developing trade programs, and enforcing U.S. import laws.

CBP has the dual mission of securing our nation's borders, while at the same time facilitating the flow of legitimate trade and travel that is so important to our nation's economy. As an agency, we protect more than 100,000 miles of shoreline and land border. We operate 330 ports of entry, and process almost 106 million cars, buses, trucks, trains, vessels and aircraft arriving at our borders each year. We screen more than 28 million commercial shipments arriving in air and maritime cargo, and 250 million more arriving in small parcels via express carriers and mail.

As America's frontline border agency, CBP plays a key role in safeguarding one of America's most valuable assets, its intellectual property (IP). According to the U.S. Chamber of Commerce, "IP-intensive industries employ nearly 18 million workers, account for more than 50% of all U.S. exports, and represent 40% of the country's growth." Thus, the theft of intellectual property poses a serious threat to America's economic vitality. But counterfeit and pirated products do more than harm the competitiveness of our industries and the employment of U.S. workers. Fake goods are capable of injuring and killing consumers and can jeopardize public safety.

In protecting America from these threats, CBP recently announced its Five-Year IPR Strategy, which was delivered to Congress in July 2010 and provides a comprehensive enforcement strategy to reduce IPR violations, including recommendations for strengthening penalties, as well as timelines for developing improved targeting models, expanding training for all enforcement personnel and expanding post-audit reviews for IPR. In addition, CBP works closely with Victoria Espinel, the U.S. Intellectual Property Enforcement Coordinator (IPEC) at the Office of Management and Budget to coordinate the U.S. government response to IPR theft, as outlined in the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (P.L. 110-403). For example, CBP collaborated with the IPEC in drafting the Joint Strategic Plan on Intellectual Property Enforcement. Moreover, CBP led an interagency working group on combating counterfeit pharmaceuticals that developed actions for the Counterfeit Pharmaceutical Interagency Working Group Report to the Vice President and Congress issued by the IPEC in March 2011. We also conducted a comprehensive review of our legal authorities

for the IPEC's White Paper on Intellectual Property Enforcement Legislative Recommendations issued in March of this year.

#### **FIVE-YEAR IPR ENFORCEMENT STRATEGY**

CBP envisions an effective IPR enforcement process in which legitimate cargo is released without delay, infringing goods are intercepted, and future violators are deterred. To achieve this vision, CBP developed the comprehensive Five-Year IPR Strategy that is underpinned by partnerships with the private sector, other agencies and foreign governments; modernized laws, technologies and processes; and a budget initiative to support investments in human capital, outreach, and technology.

CBP's IPR Strategy furthers the competitiveness of U.S. industry; supports investment in IP research and development and employment of U.S. workers; and protects American consumers, companies and national security from harm by counterfeiting and piracy. Our four-part strategy breaks down the international trade process into four main areas: 1) facilitation of the release of legitimate cargo into commerce prior to its arrival at our borders; 2) enforcement against suspect shipments when they arrive at our borders; 3) deterrence of future IP theft by counterfeiters and pirates; and 4) modernization of trade practices.

To facilitate trade and ensure compliance with IPR laws, CBP will develop partnership programs with the trade community to manage supply and distribution chains, thus enhancing IPR targeting and facilitating the clearance of compliant cargo. To strengthen

enforcement of IPR laws, CBP is developing better targeting models, expanding training for personnel involved in IPR enforcement and strengthening penalties. To advance national and economic security, CBP is engaging in cooperative efforts with other federal agencies and foreign governments to reduce international trade in counterfeit and pirated goods and to prioritize enforcement against IPR infringements with health and safety concerns, also modernizing IPR trade processes by streamlining processes and leveraging technology to more effectively enforce IPR.

#### ***FACILITATION***

Prior to the arrival of goods at our borders, CBP's objective is to identify trusted importers and legitimate shipments, allowing CBP to focus its enforcement efforts on known IPR violators and on imports for which we have less information. To accomplish this, CBP is partnering with the private sector on supply and distribution chain management programs. These programs will provide information to help us be more effective in deciding which shipments to inspect, and which to release without delay.

CBP is using risk modeling to enhance IPR targeting systems to improve the selection of shipments with a high risk of containing IPR-infringing goods for examination.

Ultimately, CBP's goal is to more effectively focus our IPR enforcement resources on those imports with a higher risk for IPR infringement, thereby increasing interdictions of IPR infringing imports and facilitating the release of low risk imports.

To do this, CBP has implemented the Center for Excellence and Expertise (CEE), a pilot program within the pharmaceutical industry that is focused on ensuring a greater degree of uniformity across ports of entry so as to remove unnecessary transactional hurdles. Through the CEE, we are collaborating with the pharmaceutical industry and gaining intelligence to segment low-risk, trusted importers from those that present higher risk for IPR violations. This allows us to facilitate entry of low-risk shipments and focus IPR enforcement resources on inspecting higher-risk shipments. CBP is also working with the pharmaceutical industry on a public awareness campaign to educate the public on the dangers posed by counterfeit drugs, including those purchased overseas and online.

Expanding trust between the private sector and CBP through trusted partner programs – supply and distribution chain management – will prove advantageous to right holders, importers and CBP. Right holders will benefit from increased protection resulting from CBP's increased targeting efficacy, and importers will experience a reduction in costs associated with unnecessary inspections and greater predictability in the processing of their shipments at the border. The additional information that will become available to CBP will improve IPR enforcement by enabling greater targeting efficacy and a corresponding increase in seizures. Lastly, improved infringement determination tools and processes will expedite the release of legitimate goods into the commerce and avoid the release of infringing goods.

***ENFORCEMENT***

When suspect goods arrive at our borders, CBP targets and inspects the goods, and seizes, forfeits and destroys counterfeit and pirated goods. CBP also enforces International Trade Commission exclusion orders, which are usually sought by patent owners. Exclusion orders enable CBP to provide protection for patented products. CBP is taking a number of steps to improve its efforts in these areas. This includes expanding IPR training for enforcement personnel and cooperating with other federal agencies and foreign governments to improve targeting and enforcement efforts.

To better equip officers in our ports of entry to enforce IPR, CBP is implementing Integrated IPR Field Training. This full-day, live, instructor-led course covers IPR policies, laws and operations. Furthermore, CBP launched a new program last year that encourages right holders to provide their product identification guides electronically to CBP. CBP makes the guides, which help us identify counterfeit and pirated products, readily available to our frontline officers in ports throughout the country. To date, CBP has received nearly 100 guides, helping us to better safeguard 1,300 trademarks and copyrights from counterfeiting and piracy.

In Fiscal Year (FY) 2010, cooperative efforts by CBP and ICE, including joint operations such as Operation Safe Summer, resulted in 19,959 seizures, an all time high and a 34 percent increase (from 14,841) in FY 2009. Included in these totals are seizures of counterfeit goods that put consumer safety and critical technology at risk, which rose dramatically due to our increased emphasis on enforcement in this area. The total

number of consumer safety and critical technology IPR seizures increased 97 percent. . The estimated manufacturer's suggested retail price (MSRP), which represents the value the seized goods would have had if they were genuine, is \$1.4 billion.

CBP is aggressively pursuing new, and strengthening existing, bilateral and multilateral engagements with foreign counterparts in order to conduct joint customs IPR enforcement operations; share effective enforcement practices; and exchange information on IPR violations to better target and interdict counterfeit and pirated goods. For example, as part of its ongoing partnership with the European Union (EU) to enforce IPR, CBP and EU customs authorities conducted the first joint customs IPR enforcement operation, Operation Infrastructure, in 2008 to target counterfeit semiconductors and computer network hardware, primarily from China. The three-week operation resulted in the seizure of more than 360,000 counterfeit components involving 40 different trademarks, most of them belonging to U.S. companies. CBP and the EU also published joint guidance for rights holders on how to work with customs authorities to protect their intellectual property.

In addition, CBP leadership currently chairs sub-committees in both the Asia-Pacific Economic Cooperation (APEC) and the World Customs Organization (WCO) and actively participates in such forums such as the U.S.-China Joint Committee on Commerce and Trade IPR Working Group. As a result of this engagement, earlier this year CBP proposed the first ever joint IPR enforcement operation among APEC customs authorities, including China, to engage in a joint operation targeting IPR violations later

this summer. Moreover, in conjunction with the U.S.-China Strategic and Economic Dialogue (S&ED), CBP has increased collaboration with China Customs on IPR enforcement to combat the prolific trade in counterfeit goods coming from China. CBP also signed a Memorandum of Understanding (MOU) with China's Ministry of Public Security during the S&ED to expand intelligence and information-sharing and increase coordinated enforcement efforts with China's enforcement agencies.

CBP also works with other federal agencies to build IPR enforcement capacity in countries around the world. We train foreign officials to increase their IPR enforcement skills and promote better IPR border enforcement to combat global trade in IPR-infringing goods.

#### ***DETERRENCE***

In conjunction with our IPR enforcement efforts directed at goods entering and exiting the United States, CBP is working proactively to deter future violations. Such initiatives include strengthening the deterrent effect of fines and penalties by appropriately levying them and increasing collections; expanding and increasing the effectiveness of IPR audits to deprive counterfeiters and pirates of their illicit profits; and promoting criminal enforcement against counterfeiting and piracy by collaborating with ICE and supporting the IPR Center.

Between FY 2006 and FY 2010, CBP increased the number of IPR penalties it assessed by 8 percent and the amount it collected by 3 percent. Cumulatively, from FY 2006 to



FY 2010, CBP assessed 514 IPR penalties and collected \$2,114,519 in fines. When collecting civil penalties, CBP is challenged by the fact that businesses who knowingly import counterfeit and pirated goods operate with minimal assets. It is often more efficient for these businesses to shut down their operations and re-open under a new name rather than to pay a fine or penalty. CBP has implemented a number of actions to address this challenge and ensure that the expenses that CBP must incur in order to collect the penalties do not exceed the amount collected.

To enhance deterrence of IPR theft, CBP is implementing new procedures for issuing civil penalties under 19 U.S.C. 1526(f). Currently, these penalties are usually issued to the U.S. importer or consignee. Under new guidelines, we will penalize persons who direct, assist financially or otherwise, or who aid and abet the importation of merchandise seized for bearing a counterfeit mark to the full extent allowed under the law.

In addition, CBP is changing its IPR penalty process so that we issue the penalties concurrently with the seizure of the counterfeit goods rather than waiting for the forfeiture proceeding to be complete, which can delay the issuance of penalties for up to two years.

In a corresponding effort, CBP is collaborating with the Department of Justice (DOJ) to identify ways to enhance the quality of IPR penalty cases and to ensure that CBP's IPR penalty cases are referred to DOJ for judicial action.

From FY 2005 through FY 2011 to date, CBP has completed 85 audits of importers at high risk for IPR violations, primarily known IPR violators. These audits have resulted in penalties, which are assessed under 19 U.S.C. § 1595a(b) and based on domestic value, of \$12.3 million for IPR infringements. Of the 85 importers audited for IPR violations, only 16 importers, or 19 percent, subsequently imported shipments of counterfeit goods. Thus, the IPR Audit Program has had the positive impact of deterring 81 percent of these importers from committing IPR violations.

CBP is a leading source of referrals to ICE for possible criminal investigation of IPR infringement. As a participating agency in the National IPR Coordination Center (IPR Center), CBP leverages our targeting and interdiction successes to contribute to special operations. For example, CBP, in conjunction with FBI and ICE, initiated Operation Network Raider in May 2010, which targets the illegal distribution of counterfeit network hardware manufactured in China. To date, referrals from this operation to ICE for criminal investigation have resulted in 30 felony convictions and 700 seizures of counterfeit Cisco network hardware. CBP is also participating in the recently announced IPR Center Operation Chain Reaction, a multi-agency effort to protect the military's supply chain from being infiltrated by counterfeit goods.

#### ***MODERNIZATION***

Increasing CBP's IPR enforcement capabilities will lead to increased interdiction of infringing goods, and deterring future violations will positively impact the economy and protect the safety and security of Americans.

As I previously noted, in June 2010, the IPEC issued the Administration's first Joint Strategic Plan on Intellectual Property Enforcement (JSP), which was developed in coordination with many federal agencies, including the Departments of Homeland Security, Justice, State, Commerce, Health and Human Services, and the U.S. Trade Representative. As part of the JSP, the Administration reviewed existing laws to ensure that they were effective and did not hinder enforcement. Based on that review, in March 2011 the Administration issued a white paper identifying specific legislative recommendations to increase the effectiveness of IPR enforcement efforts. One of these recommendations is to give DHS the authority to share information with right holders prior to the seizure of goods to help determine whether products are infringing.

This recommendation recognizes that right holders know their products better than anyone and can provide valuable information to assist CBP in determining the authenticity of suspect goods. However, CBP also has an obligation and long-standing history of providing appropriate safeguards for importers importing legitimate products. In this regard, CBP strongly supports policies providing us with the ability to share information and samples of suspected counterfeit and piratical goods with right holders in order to assist with making such a determination.

## **CONCLUSION**

Chairman Leahy, Ranking Member Grassley, and distinguished Members of the Judiciary Committee, as you know the trade in counterfeit and pirated goods threatens America's

innovation-based economy, the competitiveness of our businesses, the livelihoods of U.S. workers, our national security, and the health and safety of our consumers.

I thank you again for the opportunity to appear before you today to present an overview of CBP's actions to ensure that American intellectual property is protected and that imports comply with our nation's laws. We recognize that we have an important obligation to prevent any abuse of our open marketplace, and we take our role in this process very seriously.

I look forward to answering any questions you may have.

PREPARED STATEMENT OF ERIK BARNETT, ASSISTANT DEPUTY DIRECTOR, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC



## U.S. Immigration and Customs Enforcement

---

STATEMENT

OF

ERIK BARNETT  
ASSISTANT DEPUTY DIRECTOR

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT  
DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

“OVERSIGHT OF INTELLECTUAL  
PROPERTY LAW ENFORCEMENT EFFORTS”

BEFORE THE

UNITED STATES SENATE  
COMMITTEE ON THE JUDICIARY

Wednesday, June 22, 2011 - 10:00 a.m.  
226 Dirksen Senate Office Building

## INTRODUCTION

Chairman Leahy, Ranking Member Grassley, and distinguished Members of the Committee:

On behalf of Secretary Napolitano and Director Morton, I would like to thank you for the opportunity to highlight the important role U.S. Immigration and Customs Enforcement (ICE) plays in combating intellectual property (IP) theft in today's global economy.

Simply put, American business is threatened by those who pirate copyrighted material and produce counterfeit trademarked goods. Criminals are attempting to steal American ideas and products and sell them over the Internet, in flea markets, in legitimate retail outlets and elsewhere. From counterfeit pharmaceuticals and electronics to pirated movies, music, and software, IP thieves undermine the U.S. economy and jeopardize public safety. American jobs are being lost, American innovation is being diluted and the public health and safety of Americans is at risk – and organized criminal enterprises are profiting from their increasing involvement in IP theft.

One of the ways the Administration is responding to this organized criminal activity is through a first-of-its-kind, coordinated, and strategic offensive that targets counterfeiters and those who pirate copyrighted material. This offensive involves multiple departments and agencies within government coming together in an ICE-led task force, the National Intellectual Property Rights Coordination Center (IPR Center). IP enforcement policy across many different federal agencies is being coordinated by the first presidentially appointed, Senate-confirmed Intellectual Property Enforcement Coordinator (IPEC), Victoria Espinel, with whom ICE has the great privilege to work.

ICE and the IPR Center contributed and consulted frequently with the IPEC on the creation of the first-ever Joint Strategic Plan on Intellectual Property Enforcement, released in June 2010. Additionally, we contributed to the IPEC's 2010 Annual Report to Congress, released in February 2011, and a variety of other reports to Congress and the Vice President.

### **BACKGROUND**

America's entrepreneurial spirit and integrity are embodied by the creativity and resourcefulness of our workforce. New inventions, innovations, works of art, and discoveries create jobs and industries and add to our country's heritage. Innovation drives commerce and enables the United States to compete in the global marketplace. Intellectual property rights and the ability to protect those rights encourage American companies to continue the tradition of American innovation by developing products, ideas and merchandise.

Intellectual property rights laws protect this tradition of innovation by thwarting thieves from selling cheap imitations of products that are often far less reliable than the original products. Moreover, enforcement of intellectual property laws can support efforts to protect public safety with respect to materials that are potentially harmful. They protect our military members by preventing the spread of untested and ineffective knockoff components. Intellectual property laws also protect the actor, director, writer, musician, artist, and countless others who labor in and around America's entertainment industry from having a movie, manuscript, song or design illegally sold by someone who had no part in the artistry of creating it. Violators of laws on intellectual property rights

unfairly devalue American products and ideas, hinder our ability to grow our economy, compromise American jobs, and put consumers, families, and communities at risk.

As the members of this Subcommittee well know, globalization provides boundless opportunities for commerce, but it also brings a growing set of challenges including combating the theft of intellectual property. In a global economy, enforcement of intellectual property rights laws is crucial to ensuring that legitimate manufacturers and companies can expend capital developing overseas markets, exporting goods and creating jobs.

#### **ICE'S ROLE**

ICE has a legacy of engagement in enforcement against IP theft that spans our past as U.S. Customs Service investigators to our present role as Homeland Security Investigators. ICE is a leading agency in the investigation of criminal intellectual property violations involving the illegal production, smuggling, and distribution of counterfeit and pirated products, as well as associated money laundering violations. We target pirated and counterfeit goods entering the United States through our ports from various countries overseas. We seize the counterfeit goods that infringe trademarks, and pirated goods that infringe copyrights. In addition, we investigate the criminals engaged in IP theft. ICE has become increasingly innovative in how we combat counterfeiting and piracy. Our goal is to disrupt the manufacturing, distribution, and financing segments of criminal organizations.

ICE recognizes that no single U.S. law enforcement agency alone can succeed in the fight against IP theft. Rather, it is essential that all relevant federal agencies work



together and with industry to confront this challenge. ICE formed the IPR Center to leverage government resources to combat IP theft.

### **THE IPR CENTER**

The mission of the IPR Center is to address the theft of innovation that threatens U.S. economic stability and national security, undermines the competitiveness of U.S. industry in world markets, and places the public's health and safety at risk. The IPR Center promotes coordination and communication across the many U.S. government agencies with roles in enforcing IP laws. The IPR Center brings together key domestic and foreign investigative agencies to efficiently and effectively leverage resources, skills and authorities to provide a comprehensive response to IP theft.

The IPR Center, located in Arlington, Virginia, is an ICE-led task force of 18 relevant federal and international partners. The IPR Center includes embedded team members from, among others: U.S. Customs and Border Protection (CBP), the Food and Drug Administration Office of Criminal Investigations (FDA OCI), the Federal Bureau of Investigation (FBI), the U.S. Postal Inspection Service (USPIS), the Department of Commerce International Trade Administration, the U.S. Patent and Trademark Office, the Defense Criminal Investigative Service, the Naval Criminal Investigative Service, the Army Criminal Investigative Command Major Procurement Fraud Unit and the Inspector General's Office from the General Services Administration. In 2010, the Government of Mexico and INTERPOL joined the IPR Center as our first international partners.

Thus far in 2011, the IPR Center has welcomed the following new partners: the U.S. Consumer Product Safety Commission; the Defense Logistics Agency Office of

Inspector General; the U.S. Department of State Office of International Intellectual Property Enforcement; the U.S. Air Force Office of Special Investigations and our third international partner, the Royal Canadian Mounted Police. While the U.S. Department of Justice (DOJ) is not an official partner at the IPR Center, trial attorneys from the Computer Crime and Intellectual Property Section (CCIPS) regularly provide counsel on ongoing enforcement operations and policy. Together, the partners at the IPR Center and DOJ have created a one-stop shop for industry and victims of IP theft, reducing duplication and allowing us to leverage and benefit from our different areas of expertise.

#### **ICE'S INTERNATIONAL EFFORTS**

ICE's Homeland Security Investigations International Affairs (HSI-IA) represents the largest investigative law enforcement presence abroad for the Department of Homeland Security (DHS).

ICE attachés work with international organizations and foreign law enforcement counterparts to build capacity, strengthen relationships, and conduct joint enforcement activities. ICE is recognized as a worldwide subject matter expert on criminal customs matters, and holds the following positions at the World Customs Organization (WCO): Vice Chair for the Enforcement Committee and Chair of the Commercial Fraud Working Group. In addition, ICE and the IPR Center have repeatedly teamed with the WCO and its member countries in several multilateral enforcement operations targeting counterfeit goods.

***ICE's work in China***

The primary source country for the manufacture and distribution of counterfeit merchandise exported to the United States is China. In FY 2010, ICE and CBP seized IPR violative goods from China with a domestic value (as opposed to manufacturer's suggested retail value) of more than \$124.6 million. These seizures accounted for approximately 66 percent of the total domestic value of counterfeit merchandise seized by DHS.

ICE has a presence in central and southern coastal China with offices in Beijing and Guangzhou. These two offices have significant commercial fraud and IP portfolios. Our Assistant Attaché in Guangzhou is designated as ICE's first "IP Attaché" and is ICE's point of contact for all IP matters involving China. Moreover, the ICE office in Guangzhou is working on a U.S. Consulate project to help make Shenzhen a model IP enforcement city. ICE has made a commitment to work with the Consulate on this project and to provide training to the Chinese Public Security Bureau on IP investigation and enforcement.

On May 5, Director Morton signed a Memorandum of Understanding on Law Enforcement Cooperation in Criminal Matters with the China General Administration of Customs (GACC) Minister Yu Guangzhou. This MOU facilitates law enforcement cooperation and information sharing between ICE and the GACC, including on IP theft. This agreement follows Director Morton's trip to China last September for meetings with our Chinese law enforcement counterparts. During that trip, Director Morton signed an agreement with the Ministry of Public Security (MPS) to cooperate on joint

investigations of IP theft. The IPR Center also regularly liaises with MPS representatives from the Chinese Embassy in Washington.

These new agreements build on our previous work with China. In September 2003, ICE collaborated with Chinese authorities on Operation Spring, a joint IPR investigation that resulted in the extradition and conviction of DVD pirate Randolph Guthrie, who was sentenced to 48 months incarceration and ordered to repay \$878,793 in restitution to the Motion Picture Association of America. Another joint ICE-Chinese investigation resulted in four arrests in the United States and the seizure of more than \$100 million in counterfeit computer software and approximately \$4 million in counterfeit cigarettes.

***ICE's work in other countries***

ICE works with our Korean partners in Seoul to combat IP violations occurring in that country. In September, ICE signed a Memorandum of Understanding with the Korean Supreme Prosecutor's Office to work collaboratively on IP investigations. Since FY 2008, seizures in Korea involving our attaché in Seoul have increased dramatically: in FY 2010, 22 individuals were arrested, and merchandise valued at approximately \$18.7 million was seized. So far in FY 2011, 51 persons have been arrested and ICE has assisted in seizures valued at approximately \$16.5 million.

In July 2009, ICE opened an office in Brussels to work directly with the WCO on multilateral operations addressing bulk cash smuggling and explosives precursor chemicals. ICE also works with INTERPOL, the Asia-Pacific Economic Cooperation Forum, and the Departments of State, Commerce, and Justice on a variety of initiatives,

including providing training on IPR enforcement to our international law enforcement partners.

***ICE'S contributions to foreign training and capacity building***

The IPR Center works closely with its partner agencies, international attaché networks, and U.S. embassies to deliver training and support capacity building bilaterally and through international organizations such as the WCO and INTERPOL.

ICE provides training on IP theft enforcement and interacts with foreign officials worldwide through our participation in the Department of State International Law Enforcement Academy (ILEA) program. The mission of the ILEAs — located in Budapest, Gaborone, San Salvador, Bangkok and Lima — is to help protect U.S. interests through international cooperation and the promotion of stability by combating crime. The IPR Center recently conducted an IPR Symposium funded by the Department of State, with participation from DOJ, USPTO, and CBP, in Hong Kong for representatives from Chinese, Hong Kong, Macanese, and Malaysian law enforcement and has future Department of State-funded training planned in the Philippines.

In addition, the IPR Center supports the USPTO international training events at their Global IP Academy, and hosts visits by international law enforcement and customs officers participating in various International Visitor Programs. Through these efforts, the IPR Center is enhancing cooperation, increasing skill sets, and facilitating relationships with international partners that are critical to addressing IP theft overseas.

**STATE AND LOCAL LAW ENFORCEMENT TRAINING AND OUTREACH**

ICE and the IPR Center believe that an effective enforcement strategy must include the participation of our state, local, and tribal law enforcement partners. On World IP Day in 2010, ICE announced the creation of local IP Theft Enforcement Teams (IPTETs). The IPTETs are partnerships with state and local law enforcement built on the best practices identified by the IPR Center. They use an informal task force approach to enhance coordination of intellectual property investigations at the state, local and tribal level. There are currently 26 IPTETs across the country that include federal, state, local and tribal law enforcement partners, including sworn personnel from police and sheriff departments and local prosecutors. The IPR Center has been conducting training for the IPTETs around the country since their creation.

**PUBLIC OUTREACH**

ICE has recently taken additional steps to warn the public about the dangers and the economic impact of IP theft. To coincide with World IP Day in April, ICE teamed up with the film industry to launch a new public service announcement. The announcement highlights the effects of IP theft on American jobs, specifically focusing on the entertainment industry and its rights holders – the musician, the songwriter, the actor, the director and the countless others who labor in the entertainment industry. In just the few months since it was launched, there have been more than 115,000 views of the PSA. ICE is working to develop additional PSAs that will focus on other industries prone to IP theft.

ICE has also signed agreements with four major movie studios to place an anti-piracy warning with the IPR Center logo and ICE HSI badge on works streamed in various pay-per-view and on-demand formats. These new warnings will demonstrate ICE's role in combating IP theft and will educate the public that IP theft is a crime, not only in traditional media, but also when done through digital media.

### **RECENT ENFORCEMENT SUCCESSES**

#### ***Operation In Our Sites***

Last year, the IPR Center launched Operation In Our Sites, a new initiative targeting websites being used to sell counterfeit goods and distribute pirated merchandise and copyrighted digital materials. During the first enforcement action as part of this initiative, ICE agents, working with the U.S. Attorney's Office for the Southern District of New York, obtained judicially authorized seizure warrants and seized seven illegal domain names providing access to more than 500 movies and television programs.

On November 29, 2010, Director Morton joined the Attorney General to announce the results of Operation In Our Sites v. 2.0. Timed to coincide with "Cyber Monday," reportedly the largest online shopping day of the year, the operation targeted online retailers of counterfeit goods, including sports equipment, shoes, handbags, athletic apparel and sunglasses, as well as illegal copies of copyrighted DVD boxed sets, music and software. ICE and DOJ obtained federal court orders to seize the domain names of 77 internet sites selling counterfeit goods, five websites selling pirated movies, music and software, and one server. The operation was spearheaded by the IPR Center,

in coordination with DOJ Computer Crime and Intellectual Property Section, nine ICE field offices, and ten U.S. Attorneys' Offices.

In 2011, ICE HSI has conducted three additional rounds of Operation In Our Sites. On February 4, which coincided with the Super Bowl, ICE seized 10 domain names of websites that provided access to pirated telecasts of the National Football League (NFL), the National Basketball Association (NBA), the National Hockey League (NHL), World Wrestling Entertainment (WWE), and the Ultimate Fighting Championship (UFC). On March 3, ICE and DOJ announced the arrest of the operator of one of these websites on charges of federal copyright violation.

The domains seized pursuant to court order display a banner announcing the seizure of the site by the government and an explanation of the federal crime and punishment for copyright theft and distribution of pirated content or trademark violations. Since the initial seizures in June 2010, there have been more than 60 million hits to the banner that notifies viewers that a federal court order has been issued for the domain name and educates them that willful copyright infringement is a federal crime. After the seized domain names are forfeited to the U.S. government, a new banner is placed on the sites notifying the public that the sites have been forfeited and linking the viewers to the ICE PSA. To date, 75 of the 125 seized domain names have been forfeited. The resulting public education about IP theft is a significant benefit of this enforcement operation, and can help to deter future crimes and raise awareness.

The Operation In Our Sites initiative will continue through 2011 and beyond. ICE's efforts through this operation successfully disrupt the ability of criminals to purvey copyrighted materials illegally over the internet. In addition to the domain names that are



seized through this operation, evidence suggests that the operation has a deterrent effect. In fact, following Operation In Our Sites v. 1.0, ICE was notified that 81 of the most active websites that had been offering pirated material voluntarily shut down.

***Other notable investigative successes against IP theft***

ICE's IP theft enforcement efforts have continued to increase under this Administration. In FY 2010, ICE initiated 1,033 intellectual property infringement cases—a 42 percent increase over FY 2009—and achieved 365 arrests, 216 indictments and 170 convictions. In FY 2010, indictments flowing from ICE-initiated intellectual property investigations increased by 86 percent over the previous year. These figures include both federal and state prosecutions. The following cases illustrate some of our notable IP enforcement successes.

In the past year, ICE agents continued to seize millions of dollars in counterfeit items as a result of significant criminal investigations including an investigation into a criminal organization smuggling counterfeit shoes and luxury goods through the Port of Baltimore, with an estimated manufacturer's suggested retail price (MSRP) of more than \$219 million (had the products been legitimate goods). This investigation resulted in eight federal arrests. ICE was able to develop evidence on a parallel operation in the United Kingdom, and our ICE Attaché in London passed the information on to relevant UK law enforcement. This resulted in six arrests, seizures of 50,000 counterfeit luxury items and approximately \$617,000 in U.S. equivalent currency, making it one of the largest IP theft enforcement cases in UK history.

We have broadened our reach by partnering with foreign counterparts, such as the Mexican Tax Administration Service, which seized 306 tons of counterfeit merchandise at mail facilities and land, air and sea ports of entry during just one joint operation.

Earlier this year, the IPR Center partnered with the NFL, NBA, NHL, the National Collegiate Athletic Association (NCAA), industry and local law enforcement to conduct operations targeting counterfeit sports merchandise sold during the Super Bowl, the NBA All-Star Game, the Stanley Cup championship, and the NCAA Final Four and Frozen Four tournaments. These operations resulted in seizures of more than 21,000 counterfeit items valued at more than \$1.1 million.

In June 2010, ICE and CBP completed the U.S. portion of Operation Global Hoax, a three-month multilateral enforcement action proposed by the IPR Center and coordinated with the WCO. Global Hoax is the first-ever worldwide enforcement action targeting counterfeit DVDs and CDs as they are shipped around the world. The five-day surge operation at mail and express courier facilities resulted in the seizure of more than 140,000 pirated DVDs, 28,000 CDs, and more than 270,000 other counterfeit items worldwide. Domestically, ICE HSI and CBP seized 22,371 pirated DVDs, 2,658 pirated DVD box sets, 133 pirated CDs and 8,556 other counterfeit items worth a total MSRP of approximately \$5.3 million.

In October 2010, the IPR Center coordinated U.S. efforts in Operation Pangea III, a global operation targeting illegal pharmaceutical sales over the Internet that involved the participation of ICE, CBP, Food and Drug Administration (FDA), U.S. Postal Inspection Service (USPIS), Drug Enforcement Administration (DEA), authorities in 45 other countries, the WCO, INTERPOL, international organizations, and industry. The

U.S. operation was conducted at mail facilities in several U.S. cities. Internet monitoring revealed more than 820 websites engaged in illegal activity, including those offering controlled substances or prescription-only drugs. Nearly 300 of these websites have been taken down and investigations continue. Participants inspected approximately 278,000 packages, seizing more than 11,000 packages containing more than 2.3 million illicit and counterfeit pills worth \$6.77 million. Globally, 130 search warrants were executed and 87 individuals were arrested or are under investigation for a range of offenses.

ICE remains steadfast in its efforts to prevent IP theft from supporting those who would harm the United States or our interests abroad. In November 2009, ICE and the FBI worked with the New Jersey State Police and the Philadelphia FBI Joint Terrorism Task Force on a case that identified: a three-cell criminal organization; a U.S.-based stolen property and counterfeit goods group; an overseas procurement group; and an international group tied to Hezbollah procuring weapons, counterfeit money, stolen property, and counterfeit goods. Ultimately, the investigation resulted in 25 indictments, 16 criminal arrests, 15 administrative arrests, and 10 INTERPOL Red Notices.

#### **ICE'S PARTNERSHIP WITH THE PRIVATE SECTOR**

In addition to our investigative efforts, we are working with the IPEC and other agencies to support efforts to establish voluntary agreements with payment processors, ad networks, and other intermediaries to do the right thing. When combined with our law enforcement efforts, the private sector's voluntary action against infringers can have a tremendous effect on online crime. No one has a greater incentive for protecting intellectual property rights than private industry. Companies want to protect their

investments in research, development, manufacturing, sales, marketing and product distribution.

To help enhance and facilitate productive partnerships within both the public and private sectors, the IPR Center provides industry with valuable information about ICE's efforts to combat the importation of hazardous and counterfeit and pirated products, and it provides points of contact in ICE field offices that industry can use to provide ICE with leads and tips. For fiscal year 2009 through April 2011, the IPR Center and ICE agents have conducted approximately 604 outreach efforts, formal presentations, and meetings, in total speaking with more than 33,000 industry representatives.

#### **BUILDING PUBLIC AWARENESS ABOUT IP THEFT**

ICE believes that we can only be truly successful in our efforts against IP theft if there is a broad change in public perception regarding IP crimes. Too many individuals believe buying knock-off goods or downloading films or songs from piratical sites is a victimless crime. The public must recognize that counterfeiting and piracy is theft -- theft of innovation, jobs, and revenue that sustains jobs, advances American business and supports industrial growth and economic stability.

The IPR Center is leading an effort to educate the public and other audiences about IP theft and its connection with international organized crime. In June 2010, the IPR Center hosted a Symposium titled "IP Theft and International Organized Crime and Terrorism: The Emerging Threat." Panels of academics, industry leaders and domestic and international government officials discussed links between international organized crime, terrorism and IP theft. Attendees included congressional staff, domestic law

enforcement officials, media and others. A similar symposium on the impact of cyber crime on IP theft will be held this September.

### **CHALLENGES AHEAD**

As noted previously, ICE is working closely with international law enforcement partners to facilitate global investigations and crack down on transnational criminal organizations. However, there are more criminals engaged in IP theft than ever before, and they are counterfeiting materials and items that can affect public health and safety. As international criminal organizations have yielded huge profits through trafficking in counterfeit and pirated goods, they have extended their existing criminal infrastructures and smuggling routes to include the flow of counterfeit and pirated merchandise. Criminal penalties for commercial fraud violations as imposed are less severe than traditional drug or weapons trafficking offenses, which may contribute to the perception that IP theft is a relatively “low risk” endeavor for criminal enterprises planning to expand their operations.

Moreover, over the last 10 years, the growth of the Internet as a global commerce medium has caused it to develop into a key means for facilitating IP theft. The 2010 Cisco Visual Networking Index forecasts that global IP traffic will quadruple by 2014. In addition, Cisco notes that download speeds of DVD quality movies have been reduced from three days 10 years ago to just around two hours this year; an MP3 audio download time has been reduced from three minutes to approximately five seconds. This increase in access to the Internet, while of great benefit for global communication and commerce, presents challenges with regard to IP enforcement.

IP theft cases have also grown in both magnitude and complexity. A crime previously viewed as limited to luxury goods (such as high-priced handbags, apparel, and watches) has quickly grown to include all types of products and consumer goods at every price point, driving more challenging and involved investigations. In addition, while ocean-crossing shipping containers are necessary to move bulk quantities of counterfeit items such as handbags, shoes, batteries or holiday lights, other items including counterfeit pharmaceuticals, mobile phones, computer network components, microchips, MP3/4 Players, pirated DVDs/CDs are being smuggled in smaller and smaller quantities through mail and/or express courier parcels. ICE and CBP, using our authorities to inspect imported goods for customs violations, has engaged in successful surge operations at mail and courier facilities to generate seizures, controlled deliveries, intelligence and investigative leads.

Another challenge we face is that criminals are willing to counterfeit and pirate and market any product if it will sell, regardless of whether such sale could result in serious and significant injury to consumers or the public. ICE has investigated cases involving counterfeit toothpaste that contained a component found in antifreeze. Likewise, in 2007, ICE and the FDA arrested Kevin Xu, one of the world's most prolific counterfeiters of pharmaceuticals. Xu has been linked to distribution of counterfeit medications such as Plavix, Zyprexa, and Casodex that are used to treat blood clots, schizophrenia, and prostate cancer, respectively. In 2009, Xu was sentenced to six and a half years in prison. This April, Xu's conspirator in the United Kingdom, British citizen Peter Gillespie, was sentenced to eight years in prison for his role in this international scheme. Earlier this month, following a joint ICE HSI, FDA and USPIS case, a Chinese

national was sentenced to seven years in prison for trafficking in a counterfeit version of Alli, a weight loss drug. The drugs he trafficked contained undeclared active pharmaceutical ingredients, including Sibutramine, a non-narcotic controlled substance. One victim suffered a stroke after taking the counterfeit medication.

ICE and the FBI, along with DOJ, have also investigated the potential sale of counterfeit Cisco Gigabit Interface Converters to the U.S. Department of Defense for use by U.S. Marine Corps personnel operating in Iraq. Failure of these counterfeit devices on the battlefield would have endangered the lives of American service members. The defendant's profit would have been only approximately \$120,000, showing the callousness with which many counterfeiters treat human life. I am pleased to report one defendant in this case investigated by ICE was recently sentenced to more than four years in prison.

These cases are troubling and demand continued attention from criminal investigators and regulatory agencies. On June 14, ICE announced the beginning of Operation Chain Reaction, a joint operation between ICE, the Department of Defense, FBI, CBP, GSA and DOJ to target counterfeit parts in the Defense Department and U.S. Government supply chain. Through this operation, we will work together with our partners to protect the members of the Armed Forces, enabling them to conduct their missions without the fear that the equipment they rely on may be counterfeit. At ICE, we are prioritizing our investigative resources to focus on IP theft enforcement that protects health and safety, including the safety of our soldiers serving abroad, and supports U.S. innovation and creativity.

**CONCLUSION**

Thank you for the opportunity to appear before you today to discuss the work of ICE in enforcing U.S. intellectual property rights. I would be pleased to answer any questions that you may have at this time.



## QUESTIONS

### QUESTIONS SUBMITTED BY SENATOR TOM COBURN FOR VICTORIA ESPINEL AND ALL WITNESSES

**Questions of Senator Tom Coburn, M.D.**  
*"Oversight of Intellectual Property Law Enforcement Efforts"*  
 United States Senate Committee on the Judiciary  
 June 29, 2011

---

#### Victoria Espinel, IPEC

1. According to your March Report on the counterfeit pharmaceutical working group, several members of the Internet industry have come together to establish a private industry response to the problem of online sales of counterfeit pharmaceuticals.
  - a. What is the status of the working group as of today?
  - b. What specific actions has it taken to combat counterfeit pharmaceutical sales?
  - c. Do you feel such a private industry group would be effective at combating other types of online counterfeit websites? Why or why not?
  - d. What other types of industry working groups have been established to-date?
2. According to your 2010 Annual Report, you will be releasing a study this year on how intellectual property enforcement contributes to our economic growth. Could you explain why this study is needed and when you plan to release it?
3. In October 2010, the GAO submitted a report on the implementation of the PRO-IP Act. It provided two recommendations related to the Joint Strategic Plan. GAO recommended 1) assigning implementation of all of the plan's priorities and action items to specific agencies; and 2) providing estimates of the resources needed to carry out the priorities of the plan. What is your response to these recommendations?

#### To All Witnesses

1. Could you each explain briefly your responsibilities in IP enforcement and how you coordinate with one another?
2. How effective has the IPR Center been at coordinating agency efforts and de-conflicting cases to ensure no duplication occurs?
3. How does each of your agencies coordinate with private industry to improve your enforcement efforts?
  - a. How has the private industry stepped up their efforts to enforce their rights and coordinate with the federal government?

4. How much does each of your agencies spend annually on IP enforcement? Has that increased since the passage of the PRO-IP Act in 2008?
5. Has the amount and/or quality of agency coordination improved since the formation of the Office of the IP Enforcement Coordinator in 2009? Why or why not?
6. Are there certain products or offenses that dominate your enforcement efforts?
7. Are there certain countries that pose more serious threats to American intellectual property than others?
8. Why kind of discussions have you been having with China?
  - a. From the reports submitted by the IPEC, DOJ and FBI, it appears a majority of the cases involve Chinese products seized and/or Chinese defendants. Do you feel there has been a corresponding decrease in cases involving China since the meetings between American and Chinese officials took place last fall? Why?
  - b. What else needs to be done to decrease the infringement threat from China?

QUESTIONS SUBMITTED BY SENATOR TOM COBURN FOR JASON WEINSTEIN AND ALL  
WITNESSES

**Questions of Senator Tom Coburn, M.D.**  
*"Oversight of Intellectual Property Law Enforcement Efforts"*  
United States Senate Committee on the Judiciary  
June 29, 2011

---

Jason Weinstein, DOJ

1. Could you explain the DOJ IP Task Force and its role in coordinating DOJ's IP enforcement efforts?
  - a. How do you determine what cases to prosecute?
2. According to your 2009 and 2010 Annual Reports required by the PRO-IP Act, the DOJ did not receive funding for the grant program authorized in the bill. However, the appropriators provided funds through another program they authorized.
  - a. Under that appropriation, it appears that OJP did not award more than \$200,000 to any individual state/local law enforcement agency for IP enforcement; however, several non-profits received as much as \$600,000 to use to train state and local law enforcement. Thus, in 2009, almost half of the total grant award (\$900,000 out of a \$2 million grant) went to non-profits.
    - i. Could DOJ have provided training to state and local law enforcement on its own with less money? Why did DOJ decide NOT to do its own training?
    - ii. Has DOJ been monitoring how these non-profits are using federal funds (i.e. has the training they provide been helpful, are they using grant funds appropriately, etc.)? Why or why not?
    - iii. There appears to be a cap on how much each law enforcement grantee may receive (\$200,000). If that is true, why is there not also a cap on the amount each non-profit grantee may receive?
3. Your annual reports note DOJ also received funding under PRO-IP to hire 15 new prosecutors for its CHIP units in various U.S. Attorneys' offices. However, those reports were not clear on the total amount of funding used to hire those 15 attorneys.
  - a. How much did DOJ spend on these 15 new attorneys?
  - b. Is that the average salary of a U.S. Attorney? If not, why was a higher (or lower) amount used to hire these 15 attorneys?

To All Witnesses

1. Could you each explain briefly your responsibilities in IP enforcement and how you coordinate with one another?
2. How effective has the IPR Center been at coordinating agency efforts and de-conflicting cases to ensure no duplication occurs?
3. How does each of your agencies coordinate with private industry to improve your enforcement efforts?
  - a. How has the private industry stepped up their efforts to enforce their rights and coordinate with the federal government?
4. How much does each of your agencies spend annually on IP enforcement? Has that increased since the passage of the PRO-IP Act in 2008?
5. Has the amount and/or quality of agency coordination improved since the formation of the Office of the IP Enforcement Coordinator in 2009? Why or why not?
6. Are there certain products or offenses that dominate your enforcement efforts?
7. Are there certain countries that pose more serious threats to American intellectual property than others?
8. Why kind of discussions have you been having with China?
  - a. From the reports submitted by the IPEC, DOJ and FBI, it appears a majority of the cases involve Chinese products seized and/or Chinese defendants. Do you feel there has been a corresponding decrease in cases involving China since the meetings between American and Chinese officials took place last fall? Why?
  - b. What else needs to be done to decrease the infringement threat from China?

QUESTIONS SUBMITTED BY SENATOR TOM COBURN FOR GORDON SNOW AND ALL  
WITNESSES

**Questions of Senator Tom Coburn, M.D.**  
*"Oversight of Intellectual Property Law Enforcement Efforts"*  
United States Senate Committee on the Judiciary  
June 29, 2011

---

Gordon Snow, FBI

1. According to your 2009 and 2010 Annual Reports required by the PRO-IP Act, the FBI has used funding authorized by that Act to hire 51 new agents to work on IP enforcement-related cases.
  - a. According to the PRO-IP Act, these agents are supposed to be used for the investigation and coordination of intellectual property crimes. Do any of those agents spend time NOT working on IP cases? Why?
  - b. In 2009, FBI received \$9.4 million to hire 31 agents. \$8 million was for salaries for 31 agents and 15 support personnel, and \$1.4 million was for other funding, which included \$331,000 for travel and training of the new agents. The salary expenses are an average of approximately \$174,000 in salary per person (agents and support personnel) and \$10,677 in travel expenses per agent.
    - i. Is \$174,000 the average salary for support personnel and/or an agent? If not, what is average salary for FBI support personnel? What is the average salary for an FBI agent?
    - ii. Why was \$10,000 spent on each agent for travel? Does this amount in include conferences? If so, please break down the 2009 and 2010 travel expenses to show use of the funds.
2. How did the FBI decide where to place the 51 additional agents it has hired over the past two years? Have those agents made an impact on the number of cases opened, investigated and concluded? Why or why not?

To All Witnesses

1. Could you each explain briefly your responsibilities in IP enforcement and how you coordinate with one another?
2. How effective has the IPR Center been at coordinating agency efforts and de-conflicting cases to ensure no duplication occurs?
3. How does each of your agencies coordinate with private industry to improve your enforcement efforts?
  - a. How has the private industry stepped up their efforts to enforce their rights and coordinate with the federal government?

4. How much does each of your agencies spend annually on IP enforcement? Has that increased since the passage of the PRO-IP Act in 2008?
5. Has the amount and/or quality of agency coordination improved since the formation of the Office of the IP Enforcement Coordinator in 2009? Why or why not?
6. Are there certain products or offenses that dominate your enforcement efforts?
7. Are there certain countries that pose more serious threats to American intellectual property than others?
8. Why kind of discussions have you been having with China?
  - a. From the reports submitted by the IPEC, DOJ and FBI, it appears a majority of the cases involve Chinese products seized and/or Chinese defendants. Do you feel there has been a corresponding decrease in cases involving China since the meetings between American and Chinese officials took place last fall? Why?
  - b. What else needs to be done to decrease the infringement threat from China?

QUESTIONS SUBMITTED BY SENATOR TOM COBURN FOR ALLEN GINA AND ALL  
WITNESSES

**Questions of Senator Tom Coburn, M.D.**  
*"Oversight of Intellectual Property Law Enforcement Efforts"*  
United States Senate Committee on the Judiciary  
June 29, 2011

---

Allen Gina, CBP

1. From your testimony, it appears the process of IP enforcement begins with CBP's seizure of infringing goods. After you seize these products, how long does the forfeiture process take?
  - a. Once CBP seizes counterfeit goods, it may assess penalties in the form of monetary fines. In 2008, GAO reported that between 2001 and 2006, while CBP assessed \$1.1 billion in fines, it only collected \$2.7 million, less than 1% of the total assessed. In your testimony, you note that since 2006, increased the assessment of penalties and collection of penalties, but collection only went up by 3%. Why does CBP collect so little of the total amount of fees it assesses?
  - b. When fees are collected, where are those fees deposited? Why? Are they used to offset any of CBP's seizure costs?
2. The 2008 GAO Report also noted CBP had not been analyzing the variations in its IP enforcement activity by port, or how successful each port has been in enforcement. Does CBP now examine IP enforcement by port? Why or why not?
  - a. If you do not, how can CBP be effective in allocating its limited resources and improving the use of those resources at ports that may not be performing as they should?
3. The IPEC's 2010 Annual Report notes the number of consumer safety and critical technology seizures at CBP increased 97%. Is this because public health and safety seizures were not a priority in the past or because of more importation of these types of products? For how long have these types of seizures been a priority at CBP?
4. You note in your testimony that CBP has a Center for Excellence and Expertise, which is a pilot program focused on the pharmaceutical industry. How does this program coordinate with the IPEC's working group on counterfeit pharmaceuticals?

To All Witnesses

1. Could you each explain briefly your responsibilities in IP enforcement and how you coordinate with one another?
2. How effective has the IPR Center been at coordinating agency efforts and de-conflicting cases to ensure no duplication occurs?

3. How does each of your agencies coordinate with private industry to improve your enforcement efforts?
  - a. How has the private industry stepped up their efforts to enforce their rights and coordinate with the federal government?
4. How much does each of your agencies spend annually on IP enforcement? Has that increased since the passage of the PRO-IP Act in 2008?
5. Has the amount and/or quality of agency coordination improved since the formation of the Office of the IP Enforcement Coordinator in 2009? Why or why not?
6. Are there certain products or offenses that dominate your enforcement efforts?
7. Are there certain countries that pose more serious threats to American intellectual property than others?
8. Why kind of discussions have you been having with China?
  - a. From the reports submitted by the IPEC, DOJ and FBI, it appears a majority of the cases involve Chinese products seized and/or Chinese defendants. Do you feel there has been a corresponding decrease in cases involving China since the meetings between American and Chinese officials took place last fall? Why?
  - b. What else needs to be done to decrease the infringement threat from China?



QUESTIONS SUBMITTED BY SENATOR TOM COBURN FOR ERIK BARNETT AND ALL  
WITNESSES

**Questions of Senator Tom Coburn, M.D.**  
*"Oversight of Intellectual Property Law Enforcement Efforts"*  
United States Senate Committee on the Judiciary  
June 29, 2011

---

Erik Barnett, ICE

1. As you know, the Judiciary Committee passed the PROTECT IP Act last month in an effort to provide the federal government more tools to address the growing problem of rogue websites that are dedicated to infringing activity. Since you have not testified in the Senate on that legislation, could you please explain your position on the bill, whether it duplicates the existing Operation in Our Sites initiatives you have been performing, why you need additional authority in the bill, and whether you think the legislation will be effective in shutting down these websites.
  - a. Under the current Operation in Our Sites, on average, how many (or what percentage of) websites removed during those operations re-appear in another form after being shut down?
  - b. When conducting Operation in Our Sites, on average, how many (or what percentage of) websites are targeted because of their effect on public health and safety?
2. In 2008, GAO reported that ICE planned to move the IPR Center and its relocation would be an opportunity to return the center to its original concept and purpose. Do you believe the IPR Center has returned to an appropriate focus as an effective coordination center?
  - a. How does the IPR Center coordinate with other agencies and de-conflict cases?
  - b. Has it been successful in preventing unneeded overlap in various agencies dealing with IP enforcement? How?
3. According to reports from the Office of the Intellectual Property Enforcement Coordinator (IPEC), ICE entered into agreements with China and Korea to cooperate between enforcement agencies to combat IP crime and money laundering. What steps have those countries taken to fulfill these agreements? Do you feel these agreements have been effective to-date?

To All Witnesses

1. Could you each explain briefly your responsibilities in IP enforcement and how you coordinate with one another?
2. How effective has the IPR Center been at coordinating agency efforts and de-conflicting cases to ensure no duplication occurs?

3. How does each of your agencies coordinate with private industry to improve your enforcement efforts?
  - a. How has the private industry stepped up their efforts to enforce their rights and coordinate with the federal government?
4. How much does each of your agencies spend annually on IP enforcement? Has that increased since the passage of the PRO-IP Act in 2008?
5. Has the amount and/or quality of agency coordination improved since the formation of the Office of the IP Enforcement Coordinator in 2009? Why or why not?
6. Are there certain products or offenses that dominate your enforcement efforts?
7. Are there certain countries that pose more serious threats to American intellectual property than others?
8. Why kind of discussions have you been having with China?
  - a. From the reports submitted by the IPEC, DOJ and FBI, it appears a majority of the cases involve Chinese products seized and/or Chinese defendants. Do you feel there has been a corresponding decrease in cases involving China since the meetings between American and Chinese officials took place last fall? Why?
  - b. What else needs to be done to decrease the infringement threat from China?

## QUESTIONS SUBMITTED BY SENATOR AL FRANKEN FOR VICTORIA ESPINEL

**Hearing on "Oversight of Intellectual Property Law Enforcement Efforts"**  
**June 22, 2011****Questions for the Record from U.S. Senator Al Franken for  
Intellectual Property Enforcement Coordinator Victoria A. Espinel**

1. According to the National Association of Boards of Pharmacy, counterfeit drug sales account for approximately \$75 billion in annual global sales. Your office has done a great deal to focus on counterfeit pharmaceuticals, which can pose a serious risk to Americans' health and safety. However, other counterfeit products, such as faulty car parts, electronics, and even toys, also endanger the health and safety of Americans. How does your office prioritize cases, and what are you doing to make sure that we are targeting the most dangerous counterfeit products?
2. You have hosted meetings with private companies, including Google, American Express, MasterCard, Visa, GoDaddy, and others, to take voluntary actions against illegal online pharmacies. In your testimony, you said that you have been encouraged by the willingness of private companies to collaborate to end the distribution of counterfeit pharmaceuticals online. Are there any companies we need to be pushing to step up and do more? What can we do to encourage this collaboration to continue?
3. In February 2011, Immigration and Customs Enforcement (ICE) seized mooo.com as part of a child pornography investigation. This seizure redirected more than 84,000 subdomains to a warning that mooo.com had been seized for involvement with child pornography, despite the fact that the overwhelming majority of these subdomains only had legal content. ICE fixed what they later admitted was an inadvertent mistake, but it took several days before the site was restored and the warnings were removed. Has your office considered putting out a set of best practices or guidelines that all law enforcement can rely on to conduct due diligence before seeking a court order to shut down entire top level domains?
4. China's piracy and counterfeit goods markets are notorious. What steps can we take to put more international pressure on China to reform its intellectual property infringement problems?
  - a. During the hearing, you mentioned that the Trade-Related Aspects of Intellectual Property Rights (TRIPS) World Trade Organization (WTO) agreement was outdated and should be revised to reflect the enormous growth in intellectual property and new technologies since 1995, when TRIPS became effective. What changes would you recommend, and what other steps do you think we can take to address piracy via our trade agreements with China?

## QUESTIONS SUBMITTED BY SENATOR AL FRANKEN FOR JASON WEINSTEIN

**Hearing on "Oversight of Intellectual Property Law Enforcement Efforts"**  
**June 22, 2011****Questions for the Record from U.S. Senator Al Franken for  
Deputy Assistant Attorney General, Criminal Division, Jason Weinstein**

1. In February 2011, Senator Wyden sent a letter requesting information about Operation In Our Sites to both the Department of Justice (DOJ) and Immigration and Customs Enforcement (ICE). In May 2011, Senator Wyden received a response from DOJ that addressed a number of his questions. However, the response did not provide a clear answer to his question about domain names operating overseas in compliance with their home country's laws. DOJ has recently decided to pursue extradition against a 23-year-old British student who operated a linking site, TVShack.net, that is likely legal under UK law, because it does not host illegal content. A Spanish company, Puerto 80, is also fighting the Rojadirecta domain name seizure for similar reason. Can you explain how the Department prioritizes domain name seizures, and how the Department decides to pursue extradition in an IP case?
  - a. If we continue to seize domain names that operate legally under their home countries' laws, how can we avoid setting a bad precedent for other countries that might want to seize American domain names with legal content under U.S. law?

## QUESTIONS SUBMITTED BY SENATOR AL FRANKEN FOR ERIK BARNETT

**Hearing on "Oversight of Intellectual Property Law Enforcement Efforts"**  
June 22, 2011**Questions for the Record from U.S. Senator Al Franken for  
Assistant Deputy Director Erik Barnett**

1. In November 2010, several music sites had their domain names seized, including Dajaz1.com, OnSmash.com, RapGodFathers.com, and rmx4u.com. The site operator of OnSmash.com, a hip-hop music blog, has said the illegal music clips were given specifically to him by artists and record labels to generate publicity, and when asked, he always removed content. Other sites, like TVShack.net, host no illegal content, only link to infringing content. In all of these cases, the site operators did not receive notice prior to the domain name seizure, and they were given no opportunity to correct the infringement. By seizing an entire domain name, you are potentially disrupting access to both legal and illegal content.
  - a. Can you explain how ICE makes the decision to seize a domain name?
  - b. Is there a way that ICE could more narrowly tailor blocking orders or verify intent and content prior to seeking a blocking order?
  - c. Would a notice process which would allow domain operators to remove the illegal content prior to the domain name seizure be less effective or more difficult to implement?
2. In February 2011, ICE seized mooo.com as part of a child pornography investigation. This seizure redirected more than 84,000 subdomains to a warning that mooo.com had been seized for involvement with child pornography, despite the fact that the overwhelming majority of these subdomains only had legal content. ICE did fix what was later admitted to be an inadvertent mistake, but it took several days before the site was back up without the warnings displayed. What is ICE doing to make sure that other investigations that result in domain name seizures do not run into this sort of problem again?

QUESTIONS SUBMITTED BY SENATOR CHARLES GRASSLEY FOR ALLEN GINA

**Senator Grassley's Written Questions for Judiciary Committee Hearing "Oversight of Intellectual Property Enforcement Efforts," June 22, 2011**

**Allen Gina, Customs and Border Protection**

1. In your opinion, what has been the most successful aspect of the PRO-IP Act in achieving its goals of comprehensive intellectual property rights enforcement?
2. In your opinion, what is the greatest challenge that CBP faces with respect to IP enforcement? What is the greatest challenge that we face with respect to IP theft?
3. The PRO-IP Act increased penalties for certain intellectual property crimes. How effective have stricter penalties been in deterring intellectual property rights violations?
4. Are there any additional tools that you'd like to see enacted into law that would assist you in your efforts to protect intellectual property rights, both here and abroad?
5. The federal government has a finite number of resources to conduct its law enforcement investigations and prosecutions. Yet piracy and counterfeiting are surging all over the world, as well as online. Do you think that rights holder actions can alleviate some of the burdens on federal law enforcement and effectively combat IP theft?
6. What kinds of trends are you seeing with respect to intellectual property theft, piracy and counterfeiting? Are we able to keep up with the evolving methods and technologies utilized by IP criminals? Are the laws on the books able to keep up with the criminals?
7. In your opinion, how effective are civil penalties as an enforcement tool at the border, as opposed to criminal prosecutions by the Department of Justice?
8. Your testimony describes efforts to increase the number and severity of civil penalties. Is this proving to be a successful deterrent?
9. Are you obtaining adequate cooperation from the Chinese government with regard to your ongoing negotiations? What are the prospects for actually improving customs enforcement through these negotiations?
10. The 2010 IPEC report mentions CBP's involvement in training programs in Africa, Europe, and other nations. How extensively is CBP involved in international training programs? What is the general substance of those trainings?

QUESTIONS SUBMITTED BY SENATOR CHARLES GRASSLEY FOR ERIK BARNETT

Senator Grassley's Written Questions for Judiciary Committee Hearing "Oversight of Intellectual Property Enforcement Efforts," June 22, 2011

**Erik Barnett, Immigration and Customs Enforcement**

1. In your opinion, what has been the most successful aspect of the PRO-IP Act in achieving its goals of comprehensive intellectual property rights enforcement?
2. In your opinion, what is the greatest challenge that ICE faces with respect to IP enforcement? What is the greatest challenge that we face with respect to IP theft?
3. The PRO-IP Act increased penalties for certain intellectual property crimes. How effective have stricter penalties been in deterring intellectual property rights violations? What effect have they had on enforcement?
4. What kinds of trends are you seeing with respect to intellectual property theft, piracy and counterfeiting? Are we able to keep up with the evolving methods and technologies utilized by IP criminals? Are the laws on the books able to keep up with the criminals?
5. Walk us through the specific methods that the IPR Center uses to get input from its partners. How many more members are you hoping to add to the IPR Center?
6. What can improve the IPR Center's efficiency and cooperation? Would it improve the effectiveness of the IPR Center if CCIPS were a partner?
7. Has ICE been the subject of any civil legal action as a result of its seizures in *Operation In Our Sites* or other counterfeit goods seizures?
8. ICE recently signed a Memorandum of Understanding with the Chinese government, has two offices in China, and is engaged in significant enforcement work in Shenzhen. What else is ICE doing to obtain increased cooperation in IPR enforcement from the Chinese government?

QUESTIONS SUBMITTED BY SENATOR CHARLES GRASSLEY FOR VICTORIA ESPINEL

**Senator Grassley's Written Questions for Judiciary Committee Hearing "Oversight of Intellectual Property Enforcement Efforts," June 22, 2011**

**Victoria Espinel, Intellectual Property Enforcement Coordinator**

1. In your opinion, what has been the most successful aspect of the PRO-IP Act in achieving its goals of comprehensive intellectual property rights enforcement?
2. In your opinion, what is the greatest challenge that the IPEC faces with respect to IP theft?
3. The PRO-IP Act increased penalties for certain intellectual property crimes. How effective have stricter penalties been in deterring intellectual property rights violations?
4. What kinds of trends are you seeing with respect to intellectual property theft, piracy and counterfeiting? Are we able to keep up with the evolving methods and technologies utilized by IP criminals? Are the laws on the books able to keep up with the criminals?
5. In your opinion, in what ways has the increased FBI-DOJ partnership been productive? How can it be improved in the future?
6. What are your thoughts on how the various enforcement agencies are cooperating in the federal government's efforts to combat intellectual property theft? What can be improved?



## QUESTIONS SUBMITTED BY SENATOR ORRIN HATCH FOR JASON WEINSTEIN

Question to Jason Weinstein, Deputy Assistant Attorney General, Criminal Division  
DOJ, from Senator Orrin G. Hatch:

Throughout my service in the United States Senate, I have worked hard to promote the protection of intellectual property rights. These rights are explicitly recognized in the U.S. Constitution, by the U.S. Supreme Court, in our international trade agreements, and by our trading partners. We must ensure that ideas, inventions, artistic works, and other commercially-viable products created out of one's own mental processes continue to be protected under the law as any other tangible product or piece of real estate.

Unfortunately, we have witnessed foreign companies – and in some cases foreign governments – undermine our leadership position by stealing intellectual property from U.S. innovator companies. If we are going to be successful in combating these crimes, we need to have more vigorous criminal enforcement of our nation's intellectual property laws.

With that said, in November 2010, a federal jury in the Northern District of California ordered SAP AG, a German software company, to pay U.S.-based Oracle Corporation \$1.3 billion for copyright infringement. This is a historic copyright infringement case, which began when Oracle sued SAP in 2007 for illegally accessing Oracle's servers to download hundreds of thousands of illegal copies of Oracle's software – avoiding licensing fees and taking customers from Oracle.

Is it correct that, to date, no criminal charges have been brought against SAP?

Do you think there should be criminal enforcement in one of the largest copyright infringement cases in history where the infringing party has confessed to the infringement and a jury awarded over a billion dollars in damages?

If the DOJ does not bring criminal charges against companies like SAP, what message are we sending to other foreign infringers?

## ANSWERS

## RESPONSES OF VICTORIA ESPINEL TO QUESTIONS SUBMITTED BY SENATOR COBURN

The Honorable Senator Tom Coburn  
 United States Senate Committee on the Judiciary  
 Oversight of Intellectual Property Law Enforcement Efforts

**1. According to your March Report on the counterfeit pharmaceutical working group, several members of the Internet industry have come together to establish a private industry response to the problem of online sales of counterfeit pharmaceuticals.**

- a. What is the status of the working group as of today?**
- b. What specific actions has it taken to combat counterfeit pharmaceutical sales?**
- c. Do you feel such a private industry group would be effective at combating other types of online counterfeit websites? Why or why not?**
- d. What other types of industry working groups have been established to-date?**

Private sector cooperation is essential if we are serious about effectively addressing online sales of counterfeit pharmaceuticals. I believe that private sector voluntary actions that are practical, effective and consistent with public policy principles, including privacy protections, free speech, competition, and due process, have the potential to dramatically improve online enforcement.

In December, I announced that American Express, Discover, eNom, GoDaddy, Google, MasterCard, Microsoft, PayPal, Visa and Yahoo! had agreed to start a new non-profit organization to increase cooperation among themselves and to take voluntary action against illegal pharmaceutical sites. The group established core operating principles that include information sharing among group members and with law enforcement about fake Internet pharmacies, funding educational campaigns and expansion of information about legitimate online pharmacies. In January, the group adopted a name – the Center for Safe Internet Pharmacies (“CSIP”) – and began working on the initial corporate structure and governance documents. CSIP has confirmed those companies that will serve as founding members; by this fall they plan to hire staff to manage the day-to-day operations of the organization and establish a website.

I am pleased that these companies have shown leadership with this initiative and I am confident that similar voluntary efforts, in combination with law enforcement action and educational awareness, can be effective in combating similar Internet-related problems that involve copyrights and trademarks. My office has been convening meetings with

various Internet intermediaries and has successfully worked with the major payment processors – American Express, Discover, MasterCard, PayPal and Visa - on a set of voluntary best practices to investigate complaints and remove payment services from any site that continues to operate unlawfully. These best practices are now final and operational and we will watch with interest in order to gauge the effectiveness of this process. We understand that Google has a payment processing arm and have asked them to consider joining this effort as well. We are also working with companies that advertise online and companies that sell online ads (ad brokers) including AOL, Bing, Google, and Yahoo to develop best practices to keep the ads of legitimate companies from financially supporting or lending legitimacy to sites engaged in infringement.

**2. According to your 2010 Annual Report, you will be releasing a study this year on how intellectual property enforcement contributes to our economic growth. Could you explain why this study is needed and when you plan to release it?**

The Department of Commerce, in consultation with the White House Council of Economic Advisors and the chief economists of many Federal agencies, is conducting an economic analysis to identify the industries that most intensively produce intellectual property, and to measure the importance of those industries to the U.S. economy. This will be the first time that the U.S. Government has conducted a broad study of this sort across all sectors of our economy. We believe that improved measures of intellectual property linked to measures of economic performance will help the U.S. Government understand the role and breadth of intellectual property in the American economy and inform policy and resource decisions related to intellectual property enforcement. On June 15, IPEC and Commerce met with a broad range of outside stakeholders to discuss the methodology of the report. We hope to finalize and release the report and the underlying data before the end of the year.

3. **In October 2010, the GAO submitted a report on the implementation of the PRO-IP Act. It provided two recommendations related to the Joint Strategic Plan. GAO recommended 1) assigning implementation of all of the plan's priorities and action items to specific agencies; and 2) providing estimates of the resources needed to carry out the priorities of the plan. What is your response to these recommendations?**

I have worked very closely with the agencies with intellectual property responsibility on the Joint Strategic Plan (Strategy) and its implementation. Specific focus has been placed on each agency's mission and efficient use of resources to accomplish the Strategy's priorities and action items. To the extent practicable, the Strategy identified specific agencies that were responsible for implementing the priorities and action items, a fact that the GAO report acknowledged. Some priorities and action items were broad in scope and warranted a government-wide approach, which I have been coordinating since the issuance of the Strategy. Consistent with the 2010 Strategy and the GAO recommendation, future Joint Strategic Plans will continue to identify specific agencies that are responsible for implementing the priorities and action items of those plans where appropriate.

With respect to GAO's second recommendation, the Strategy was carefully planned to ensure that the action items can be implemented given current resources and with shifts in processes and prioritization of the intellectual property enforcement mission. In order to gauge what we are spending now and to better inform future resource allocation, in April 2010 and 2011, we collected data on resources expended by agencies with intellectual property enforcement responsibility, including the Departments of Justice (DOJ), Commerce, State, Homeland Security, Treasury, Health and Human Services, Agriculture and the Office of the U.S. Trade Representative (USTR). Due to shifts in the enforcement landscape, some priorities and action items will require additional resources, and some agencies have requested increased funding for intellectual property priorities in the President's FY2012 budget. For instance, DOJ requested an additional \$4.8 million for 6 attorney positions to support international intellectual property criminal enforcement. Similarly, the U.S. Patent and Trademark Office (USPTO) and USTR have requested an additional \$1.1 million and \$142,000, respectively for additional personnel, including stationing personnel overseas. We will continue to work within the Administration's budget process to identify and request funding for items that will make a significant impact on intellectual property enforcement.

RESPONSES OF VICTORIA ESPINEL, JASON WEINSTEIN, GORDON SNOW, ALLEN GINA,  
AND ERIK BARNETT TO QUESTIONS SUBMITTED BY SENATOR COBURN

To All Witnesses

**1. Could you each explain briefly your responsibilities in IP enforcement and how you coordinate with one another?**

The IPEC office was created to make the government's efforts more efficient and effective in protecting people who innovate and create. My job is to work with the various agencies in the federal government and other offices in the White House to make sure intellectual property laws are enforced and working properly.

The U.S. Government as a whole has been working efficiently to tackle intellectual property enforcement issues. My office coordinates through a variety of formal and informal means, including daily correspondence and regular calls with the enforcement agencies, as well as more formal interagency meetings. With the passage of the Prioritizing Resources and Organization for Intellectual Property Act of 2008, Congress created an interagency intellectual property enforcement advisory committee, which has been helpful in coordinating these efforts. Furthermore, on February 8, President Obama signed Executive Order 13565, establishing a Cabinet-level advisory committee, chaired by IPEC, comprised of the heads of the departments responsible for intellectual property enforcement.

A key tool to improve agency coordination has been the establishment of four interagency working groups concerning U.S. Government procurement, U.S. Government personnel stationed overseas, international training efforts, and counterfeit pharmaceuticals. These working groups have used a collaborative approach to tackling enforcement issues identified in the June 2010 Joint Strategic Plan on Intellectual Property Enforcement, which has increased the amount and quality of coordination between the agencies. For example:

- The procurement working group is charged with developing legislative, regulatory and policy recommendations for President Obama to eliminate counterfeit products in the U.S. Government supply chain.
- The overseas personnel working group identified 17 countries as priority countries for intellectual property enforcement and recommended that U.S. embassies in each of those countries establish senior-level interagency working groups. The working groups have now been established and each working group has completed detailed work plans setting out the actions that embassy personnel will take to address the specific challenges in each country.

- The international training working group was formed to improve interagency coordination of international capacity building and training. As a result of this group's work, in March, the U.S. Patent and Trademark Office launched a publicly-accessible, online database that will lead to more efficient use of resources by allowing different agencies to share materials and avoid duplicative work.
- Last March, the counterfeit pharmaceutical working group presented a strategy to the Vice-President and to Congress that detailed how the U.S. Government would fight counterfeit drugs including from illegal online pharmacies. The group is now working on implementation of that strategy.

The National Intellectual Property Rights (IPR) Coordination Center, hosted by U.S. Immigration and Customs Enforcement (ICE), is another excellent example of regulatory agencies and law enforcement bodies coordinating with each other to fight intellectual property crimes. The IPR Center uses the expertise of its member agencies, also working closely with the Department of Justice's Computer Crime and Intellectual Property Section to share information, develop initiatives, coordinate enforcement actions, and conduct investigations related to intellectual property theft. Examples of these coordinated efforts include:

- The IPR Center has been making sure resources do not overlap, by working with the FBI and other IPR Center partners to de-conflict investigative activity, and their efforts have been effective. The de-confliction process has been collaborative and complementary, using each agency's comparative advantage to most efficiently conduct investigations.
- Over the past year, the IPR Center has added even more partners, including the State Department, the Consumer Product Safety Commission (CPSC), the Army Criminal Investigation Command – Major Procurement Fraud Unit, and the Defense Logistics Agency – Investigations Division. The IPR Center also added its second foreign government partner, the Royal Canadian Mounted Police, which joined the first foreign government partner, the Government of Mexico's Tax Administration Service, and added its first international law enforcement organization, INTERPOL.
- The FBI has improved the coordination of intelligence of global intellectual property threats through its Intelligence Fusion Group (IFG). The IFG, in collaboration with IPR Center partners, examines and defines the intellectual property rights threat, shares intelligence, issues intelligence reports and develops strategies for addressing intellectual property crimes.

- The FBI's Intellectual Property Rights Unit (IPRU), stationed at the IPR Center, is staffed by five full-time FBI agents who conduct complex intellectual property investigations and work with IPR Center partners to de-conflict intellectual property cases.
- ICE and the FBI have formed 30 law enforcement teams that include federal, state and local law enforcement coordinated across the country to fight intellectual property crime.

The DOJ Bureau of Justice Assistance (BJA) grant program has bolstered the coordination efforts of state and local authorities to enforce intellectual property rights. Taken together, the program grantees have seized over \$195 million worth of infringing merchandise since October of 2009 - 30 times the value of the grants (\$6.5 million) distributed to date. This is an excellent example of federal, state and local authorities working together to make a significant impact on intellectual property enforcement and we expect to see similar success in the future.

Federal, state and local authority coordination has also had positive effects beyond our borders as various agencies demonstrated in February with the extradition from Paraguay of a fugitive who allegedly supported the terrorist group Hezbollah with profits from counterfeit goods. A wide range of Federal, state, and local law enforcement agencies coordinated on that case including the FBI, ICE, Homeland Security Investigations (HSI), the New Jersey State Police, the Internal Revenue Service, the U.S. Secret Service, Defense Criminal Investigative Services, the Department of Commerce, the U.S. State Department, U.S. Customs and Border Protection (CBP), the Bureau of Alcohol, Tobacco, and Firearms and Explosives, Federal Air Marshals, Pennsylvania State Police, and the Philadelphia Police Department.

Federal agencies have demonstrated significant commitment to the goals of the Administration on enforcement of intellectual property. The Joint Strategic Plan on Intellectual Property Enforcement that we issued on June 22, 2010 reflected the cooperative efforts of agencies. Since then, we have documented our continuing progress in reports to Congress issued in February and June of this year.



**2. How effective has the IPR Center been at coordinating agency efforts and de-conflicting cases to ensure no duplication occurs?**

The IPR Center has done an excellent job of leveraging the diverse resources of the federal government into an effective force for fighting intellectual property crime. The Center works with a broad spectrum of regulatory agencies and law enforcement bodies including U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, Federal Bureau of Investigation, Food and Drug Administration's Office of Criminal Investigations, U.S. Postal Inspection Service, U.S. Department of Commerce's International Trade Administration, U.S. Patent and Trademark Office, Naval Criminal Investigative Service, Defense Criminal Investigative Service, U.S. Army Criminal Investigative Command's Major Procurement Fraud Unit, General Services Administration's Office of Inspector General, Consumer Product Safety Commission, Defense Logistics Agency, U.S. Department of State's Office of International Intellectual Property Enforcement, INTERPOL, the Government of Mexico's Tax Administration Service, and the Royal Canadian Mounted Police. Through the Criminal Division's Computer Crime and Intellectual Property Section, DOJ also provides support to the IPR Center. The IPR Center has been making sure resources do not overlap, by working with the FBI and other IPR Center partners to de-conflict investigative activity, and their efforts have been effective. The de-confliction process has been collaborative and complementary, using each agency's comparative advantage to most efficiently conduct the investigation.

**3. How does each of your agencies coordinate with private industry to improve your enforcement efforts?**

Our 2010 Joint Strategic Plan (Strategy) committed to transparency in the development of enforcement policy, information sharing and reporting of law enforcement activities at home and abroad. I have traveled to Los Angeles, Silicon Valley, Illinois and New York and will continue to travel to different parts of the country to hear stakeholder concerns directly. My office is small, but we regularly meet with hundreds of stakeholders, including companies across an extremely broad range of sectors. We have met with book publishers, movie studios, music companies, videogame companies, software development companies, fashion houses, pharmaceutical manufacturers, aerospace companies, automobile companies, electronic component manufacturers, the biotech industry, green technology innovators, telecommunications companies, textile manufacturers, jewelers, writers, programmers, artists, inventors, Internet service providers, Internet search companies, Internet auction companies, advertisers, ad brokers, credit card companies, payment processors, think tanks, consumer advocacy groups, unions, students, academics, and other intellectual property stakeholders.

In addition to meetings, my office receives input from more formal mechanisms such as federal register notices (FRN). In preparation for developing the Strategy, my office published a FRN which produced significant input from the public with over 1,600 comments and suggestions from a broad array of Americans with specific and creative ideas. Recently, we published a FRN seeking public input regarding the dangerous presence of counterfeit products in the U.S. Government supply chain. These interactions have helped us to learn about the problems American companies face, provided a range of views on policy matters related to intellectual property enforcement, and led to solutions the Administration can pursue through agency action, legislative recommendations, or other approaches.

We have also worked with, and encouraged right holders and many different companies that benefit from or facilitate e-commerce to reach cooperative voluntary agreements to reduce infringement in a practical and effective manner consistent with important public policy principles, including privacy protections, free speech, competition and due process. The first success from this approach occurred in December when American Express, Discover, eNom, GoDaddy, Google, MasterCard, Microsoft, PayPal, Visa, and Yahoo! agreed to start a new non-profit organization to increase cooperation among themselves and to take voluntary action against illegal pharmaceutical sites. The non-profit organization is called The Center for Safe Internet Pharmacies (CSIP) and they are working on developing their initial corporate structure, hiring plans and establishing a website which they hope to complete by this fall.

My office has also successfully worked with the major payment processors – American Express, Discover, MasterCard, PayPal, and Visa – on a set of voluntary best practices that are now final and operational to investigate complaints and remove payment services from any site that continues to operate unlawfully.

We welcome the July 7, 2011 agreement between Internet service providers and content providers as a cooperative effort to combat online infringement. We continue to work with other Internet stakeholders, such as advertisers and ad brokers to develop voluntary best practices to keep ads of legitimate companies off of sites that engage in infringing activity.

**a. How has the private industry stepped up their efforts to enforce their rights and coordinate with the federal government?**

Private industry has been working to enforce their rights and coordinate with the Federal government. They have assisted investigations and prosecutions of intellectual property crimes with witnesses, investigators, and other staff who have been working with the agencies to provide leads and other assistance that build and win cases. For example, pharmaceutical company agents tipped off law enforcement about sales of counterfeit pills from their undercover operations; this lead formed the basis of an investigation and guilty plea in connection with the sale of over 45,000 counterfeit pills.

Private industry has also trained U.S. Customs and Border Protection (CBP) at the ports and headquarters on how to distinguish their goods from infringing articles. CBP's Center for Excellence and Expertise is also educating more right holders on how to better enforce their rights specifically for pharmaceutical products, and the pharmaceutical industry is aiding CBP by providing advice on tracking illegal pharmaceutical shipments. The FBI and ICE have been conducting outreach and developing education programs for industry representatives with a stake in intellectual property enforcement.

Finally, DOJ's Computer Crime and Intellectual Property Section (CCIPS) organized and led approximately 10 conferences in the past four years which brought together right holders and federal, state, and local prosecutors to discuss aspects of intellectual property crime with federal law enforcement experts as well as businesses, private investigators, and corporate counsel. These conferences provide a forum for private industry to share information, ideas, and trends that they encounter with their intellectual property and can assist law enforcement to adjust their tactics accordingly.

**4. How much does each of your agencies spend annually on IP enforcement? Has that increased since the passage of the PRO-IP Act in 2008?**

IPEC spent \$230,949 in 2010. That covered the IPEC's salary and benefits, the salary and benefits of the office's confidential assistant, and the entire cost of the office's travel, furniture, IT equipment, supplies, and subscriptions. The IPEC expenditures have not increased since the passage of the PRO-IP Act in 2008.

**5. Has the amount and/or quality of agency coordination improved since the formation of the Office of the IP Enforcement Coordinator in 2009? Why or why not?**

Yes, both the amount and the quality of agency coordination have improved. Since the passage of the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act) and the introduction of the Joint Strategic Plan in June 2010, the Administration has made significant progress on intellectual property enforcement coordination in several areas including law enforcement, education/training, and interagency cooperation. Congress' creation of an interagency intellectual property enforcement advisory committee in the PRO-IP Act was an important step in increasing the amount and quality of agency coordination. President Obama took additional steps to increase agency coordination by establishing a Cabinet-level intellectual property advisory committee, chaired by the IPEC, comprised of the heads of the departments responsible for intellectual property enforcement.

In addition, my office established and chairs four interagency working groups concerning U.S. Government procurement, U.S. Government personnel stationed overseas, international training efforts, and counterfeit pharmaceuticals. These working groups have greatly increased the amount and quality of coordination between agencies.

- Recent reports issued by the Department of Commerce and the Government Accountability Office have found that counterfeits have infiltrated many sectors of the U.S. Government supply chain and have the potential to cause serious disruptions in national defense, critical infrastructure, and other vital applications. The procurement working group is made up of 14 government components and is charged with formulating legislative, regulatory and policy recommendations to President Obama to eliminate counterfeit products in the government supply chain.
- The overseas personnel working group identified 17 countries as priority countries for intellectual property enforcement and recommended that U.S. embassies in each of those countries establish senior-level interagency working groups. The working groups have now been established and each working group has completed detailed work plans setting out the actions that embassy personnel will take to address the specific challenges in each country.
- The international training working group was formed to improve interagency coordination of international capacity building and training. As a result of the group's work, in March, the USPTO launched a searchable database where agencies can post information on intellectual property enforcement trainings that will allow agencies to use resources more efficiently, improve training results and increase transparency and public participation.

- In March, the counterfeit pharmaceutical working group issued a strategy that detailed how the U.S. Government would fight counterfeit drugs and illegal online pharmacies. The group is now working on implementation of that strategy.

This activity is in addition to the daily agency coordination this office does by reaching out to multiple U.S. Government personnel to inform, discuss, and decide on the best approaches to intellectual property enforcement among the agencies. From these dialogues, we fine tune the Administration's approach on legislative recommendations, policy proposals, interagency initiatives, and other decisions that affect multiple U.S. Government agencies with intellectual property interests.

Law enforcement has also improved the amount and quality of coordination. In particular, the National Intellectual Property Rights (IPR) Coordination Center – hosted by U.S. Immigration and Customs Enforcement (ICE) – has done an excellent job de-conflicting agencies and optimizing the distribution of agency assets. For example:

- The FBI, through its Intelligence Fusion Group (IFG), has examined and assessed the intellectual property rights threat and shared intelligence assessments with its IPR Center partners. They have also deployed their Intellectual Property Rights Unit (IPRU) within the IPR Center to assist with de-confliction of cases and conduct complex intellectual property crime investigations. The de-confliction process has been collaborative and complementary, using each agency's comparative advantage to most efficiently conduct investigations.
- The IPR Center is also growing and expanding its reach by adding additional partners including the State Department, the Consumer Product Safety Commission (CPSC), the Army Criminal Investigation Command – Major Procurement Fraud Unit, and the Defense Logistics Agency – Investigations Division. The IPR Center also added its second foreign government partner, the Royal Canadian Mounted Police, who joined the first foreign government partner, the Government of Mexico's Tax Administration Service, and added its first international law enforcement organization, INTERPOL. This expansion will increase coordination and strengthen intellectual property enforcement efforts here and abroad.
- Federal, state and local law enforcement have teamed up to combat intellectual property crimes throughout the country as evidenced by the 26 ICE-lead Intellectual Property Theft Enforcement Teams (IPTETs) and the 4 FBI-lead Intellectual Property Task Forces. For example, the Houston IPTET had three significant enforcement actions over a four-month period. In July, it seized nearly a half million dollars' worth of counterfeit goods at a local boutique; in September, it seized more than \$1 million of pirated DVDs at a local flea market; and, in October, it seized \$2.5 million of counterfeit goods at three local businesses. Also, the FBI in California worked with the Placer County Sheriff's Office and Galt Police Departments on an investigation that lead to the arrest and

subsequent conviction of a defendant trafficking in a range of counterfeit items with an estimated retail value of over \$7 million, including some bearing the “UL” safety mark. In November, the defendant was sentenced to 26 months in prison, and was ordered to pay a \$25,000 fine and \$9,575 in restitution.

The DOJ Bureau of Justice Assistance (BJA) grant program has bolstered the efforts of state and local authorities to enforce intellectual property rights. Taken together, the program grantees have seized over \$195 million worth of infringing merchandise since October of 2009 - 30 times the value of the grants (\$6.5 million) distributed to date. This is an excellent example of federal, state and local authorities working together to make a significant impact on intellectual property enforcement and we expect to see similar success in the future.

Federal, state and local authority coordination has also had positive effects beyond our borders as various agencies demonstrated in February with the extradition from Paraguay of a fugitive who allegedly supported the terrorist group Hezbollah with profits from counterfeit goods. A wide range of federal, state, and local law enforcement agencies coordinated on that case including the FBI, ICE, Homeland Security Investigations (HSI), the New Jersey State Police, the Internal Revenue Service, the U.S. Secret Service, Defense Criminal Investigative Services, the Department of Commerce, the U.S. State Department, U.S. Customs and Border Protection (CBP), the Bureau of Alcohol, Tobacco, and Firearms and Explosives, Federal Air Marshals, Pennsylvania State Police, and the Philadelphia Police Department.

**6. Are there certain products or offenses that dominate your enforcement efforts?**

Many problems confront intellectual property enforcement today and my office is working hard to address each of these threats – financial, safety, or otherwise – to important sectors of the U.S. economy, including aerospace, automobile, electronic components, biotechnology, green technology, manufacturing, software, hardware, pharmaceuticals, telecommunications, military products, education, healthcare, movies, music, video games, entertainment, finance, fashion, publishing, as well as the upstream and downstream industries and people who make their living supporting or using the products and services of these innovators.

The primary concerns that drive our enforcement efforts are creating jobs, increasing exports, supporting innovation, maintaining our global competitiveness, and the health and safety of the American people. A few areas of specific focus that I would highlight include: counterfeit drugs, along with other counterfeit goods, that can cause harm to consumers, counterfeit goods in the military and government supply chains, the theft of trade secrets and innovative technology, online infringement, and intellectual property enforcement, including patent enforcement, abroad but especially in China.



**7. Are there certain countries that pose more serious threats to American intellectual property than others?**

Twelve countries—Algeria, Argentina, Canada, Chile, China, India, Israel, Indonesia, Pakistan, Russia, Thailand, and Venezuela—are listed on the Priority Watch List in this year’s USTR Special 301 Report. Priority Watch List countries are those that have the “most onerous or egregious acts, policies, or practices” that deny adequate intellectual property rights or equitable market access for persons that rely on intellectual property protection.

Of these twelve countries, China stands out. China is the top source country of intellectual property-infringing products seized by the U.S. Department of Homeland Security in FY2010, accounting for 66 percent of the total value of all intellectual property seizures during that year. In terms of monetary losses, U.S. companies in intellectual property-intensive industries report that China’s intellectual property infringement caused them approximately \$48 billion in losses in 2009, according to the U.S. International Trade Commission.

China’s unacceptable levels of retail and wholesale counterfeiting are noted in the USTR’s Special 301 Report, including persistently high-levels of book and journal piracy, end-user piracy of business software, and copyright piracy over the Internet. With regard to counterfeiting, China’s global manufacturing capacity also extends to all phases of the production and global distribution of counterfeit goods, including: apparel and footwear, mobile phones, pharmaceuticals and medical equipment, herbal remedies, wine and liquor, other beverages, agricultural chemicals, electronic components, computer and networking equipment, software and related products, batteries, cigarettes, cosmetics, home appliances, cement, and auto parts, as well as merchandise based on copyrighted works.

Piracy over the Internet in China continues to be a source of concern and injury to the copyright industries and the United States. As noted in the Special 301 Report, it is estimated that there are 457 million Internet users in China (as compared with 223 million in the United States), and that 99 percent of all music downloads in China are reported to be illegal. The Special 301 Report also recognizes industry concerns regarding China’s “indigenous innovation” policies—a set of regulations, rules and practices in a variety of fields that might be used to unfairly favor domestic Chinese intellectual property over foreign intellectual property, including preferences given to products embodying domestically-developed intellectual property in government procurement and standard setting.

Finally, there have been repeated and troubling instances of Chinese nationals and other individuals attempting to steal U.S. proprietary business information and sending that information to competitors in China. For example, in a case prosecuted by the U.S. Attorney’s Office for the Eastern District of Michigan, a Chinese national was sentenced in April to 70 months in Federal prison for misappropriating confidential design documents owned by Ford Motor Co. worth between \$50 – 100 million. In a case

prosecuted by the U.S. Attorney's Office for the District of New Jersey, a defendant was convicted in April 2011 of stealing confidential and proprietary business information—which he sent to China—for a database system with environmental uses, including hazardous waste management.

**8. What kind of discussions have you been having with China?**

President Obama, Vice President Biden, Attorney General Holder, Secretaries Geithner and Locke, U.S. Trade Representative Ron Kirk, U.S. Immigration and Customs Enforcement Director John Morton, U.S. Customs and Border Protection Commissioner Alan Bersin, Under Secretary of State Robert Hormats, and other senior Administration officials have directly and repeatedly pressed China and other countries to do much more to combat intellectual property theft.

In October I traveled to China, with Attorney General Holder, and met with Chinese officials, where I stressed the need for China to strengthen its enforcement of intellectual property rights and encouraged greater cooperation and information-sharing in cross-border intellectual property investigations with U.S. officials. Following that trip, I had discussions with senior Chinese officials on various intellectual property enforcement issues, including software legalization by China in the lead up to President Hu's state visit to Washington, DC in January of this year. Moreover, I work closely with U.S. agencies – including USTR, State, Commerce, Justice, and DHS – to ensure that the Administration's efforts are coordinated when the agencies engage China on intellectual property issues.

- a. From the reports submitted by the IPEC, DOJ and FBI, it appears a majority of the cases involve Chinese products seized and/or Chinese defendants. Do you feel there has been a corresponding decrease in cases involving China since the meetings between American and Chinese officials took place last fall? Why?**

The meetings between American and Chinese law enforcement officials have resulted in the signing of memoranda to increase information-sharing between American and Chinese law enforcement agencies. Because most of these memoranda were signed in May, it is too early at this time to determine whether there has been a statistically significant change in the number of cases involving China, which may now be under investigation but not yet publicly announced, and which are attributable to the recent information-sharing agreements between our two countries.

- b. What else needs to be done to decrease the infringement threat from China?**

The wide variety of issues and the tremendous scale of intellectual property infringement in China mean that we must address enforcement there on multiple fronts. The United States will continue to press China, directly and repeatedly, at the

most senior levels of the U.S. Government on the need for China to strengthen its intellectual property enforcement.

The Administration is pursuing a coordinated strategy, in accordance with the 2010 IPEC Joint Strategic Plan, to press China to do more to enforce intellectual property rights, including the following:

- China's Special IPR Campaign: Using the coordinated framework described in the IPEC Joint Strategic Plan section "*Enforcing our Rights Internationally*," we are working with the U.S. Trade Representative, other Federal agencies, and U.S. businesses to assess China's progress (and to encourage further action) under China's "Special Campaign Against Piracy and Counterfeiting," which China's State Council launched in October 2010 and extended through the end of June 2011. The Special IPR Campaign has resulted in improved coordination between China's intellectual property enforcement agencies and higher levels of enforcement activity in some areas. But more is needed, and we will continue to urge China, through trade dialogues such as the U.S.-China Joint Commission on Commerce and Trade (JCCT), to maintain a long-term, high-level focus on intellectual property enforcement and to continue its interagency coordination of IP enforcement at senior political levels, as they did during the Special IPR Campaign.
- Special 301 Report: This year, China was again listed on USTR's annual Special 301 Report as a Priority Watch List country. This list is reserved for countries with the most onerous or egregious acts, policies, or practices harming U.S. intellectual property owners. This year, in accordance with the IPEC Joint Strategic Plan action item "*Strengthen Special 301 Action Plans*," the USTR's Special 301 Report includes an open invitation to all trading partners listed in the report to cooperatively develop action plans to resolve IPR issues of concern. Agreement on such a plan will not by itself change a trading partner's status. However, in the past, successful completion of action plans has led to the removal of trading partners such as Saudi Arabia, Taiwan, and many others from Special 301 lists.
- Notorious Markets List: In February 2011, as part of the IPEC Joint Strategic Plan action item "*Identify Foreign Pirate Websites as Part of the Special 301 Process*," USTR released the first-ever out-of-cycle Notorious Markets List—a list of physical and online overseas markets that traffic in infringing products, including several markets in China. The list helps to raise public awareness of online piracy and counterfeiting and to focus our diplomatic efforts with China. For example, Taobao.com, China's leading business-to-consumer website (and the

fifth most-visited site in China), announced in response to having been listed in the Notorious Markets List, that it will launch a major campaign to stop online piracy and counterfeiting occurring on its site. In addition, the Government of Hong Kong took quick action against a market listed in the report, utilizing a new enforcement strategy, including increased patrols, arrests and prosecutions, and displaying an anti-piracy banner, at the notorious “Ladies’ Market.” In July, Baidu, a leading Chinese search engine listed in the report, concluded a music licensing agreement with One-Stop China, a joint venture between the Universal Music Group, the Warner Music Group, and Sony BMG.

- Building Alliances with Chinese Law Enforcement: Ultimately, we need Chinese law enforcement to do more. Both the Attorney General and DHS ICE Director Morton have traveled to China to press their counterparts for increased cooperation to fight intellectual property crime. (This is the first time an ICE director has traveled to mainland China, and Director Morton made intellectual property enforcement a major focus of his trip.) In addition, as part of the IPEC Joint Strategic Plan action item “*Enhance Foreign Law Enforcement Cooperation*,” we are working with foreign law enforcement to do more by having U.S. law enforcement on the ground working closely with Chinese law enforcement – building relationships that will lead to increased enforcement. To do so, we have been working with DOJ, FBI, and ICE to have IP-focused law enforcement personnel on the ground in China. In September 2010, the ICE Assistant Attaché in Guangzhou was designated as ICE’s first “IP Attaché” in China. The FBI is also preparing to send an IP -dedicated attaché to China later this year. In addition, the DOJ’s Criminal Division and the Chinese Ministry of Public Security (“MPS”) co-chaired the Intellectual Property Criminal Enforcement Working Group (“IPCEWG”) of the U.S.-China Joint Liaison Group for Law Enforcement Cooperation (“JLG”), which has resulted in an open dialogue on intellectual property criminal enforcement issues, increased information sharing on selected investigations, and a number of successful joint intellectual property operations.
- Software Legalization: China recently made several commitments to ensure that its government agencies and State Owned Enterprises (SOEs) use only legitimate software. These commitments were achieved and are now being monitored under the IPEC Joint Strategic Plan action item “*Promote Enforcement of U.S. Intellectual Property Rights through Trade Policy Tools*.” For example, during the 2<sup>1st</sup> JCCT in December 2010, China promised to allocate current and future budgets for purchasing, upgrading, and replacing agency software. At this meeting, China also announced that thirty SOEs will participate in a pilot project to encourage these SOEs use only legitimate software. During President Hu

Jintao's state visit in January 2011, China committed to conduct audits to ensure that government agencies at all levels use legitimate software and to publish the auditing results as required by China's law. We are now closely monitoring China's efforts to ensure that these commitments are fully implemented and that its agencies and SOEs pay for the software they use.

- Educating U.S. Small- and Medium-sized Entities: Key to increasing U.S. exports is the protection of intellectual property rights in China and the Administration's efforts to assist U.S. companies as they contemplate entering the Chinese market. Under the IPEC Strategic Plan action item "*Support U.S. Businesses in Overseas Markets*," the Department of Commerce's International Trade Administration hosts the "Intellectual Property Rights in China Webinar Series," a free webinar series for U.S. small- and medium-sized entities considering doing business in China. So far this year, eight webinars have been conducted on China-specific IP topics, including bad-faith trademark registrations, domain names disputes, and indigenous innovation. These webinars are available for viewing at [www.stopfakes.gov](http://www.stopfakes.gov). In addition, the U.S. Patent & Trademark Office each year conducts a "USPTO China Road Show," a series of free, two-day seminars for U.S. businesses to learn how to protect against intellectual property theft from China.

## RESPONSES OF VICTORIA ESPINEL TO QUESTIONS SUBMITTED BY SENATOR FRANKEN

**The Honorable Senator Al Franken  
United States Senate Committee on the Judiciary  
Oversight of Intellectual Property Law Enforcement Efforts**

- 1. According to the National Association of Boards of Pharmacy, counterfeit drug sales account for approximately \$75 billion in annual global sales. Your office has done a great deal to focus on counterfeit pharmaceuticals, which can pose a serious risk to Americans' health and safety. However, other counterfeit products, such as faulty car parts, electronics, and even toys, also endanger the health and safety of Americans. How does your office prioritize cases, and what are you doing to make sure that we are targeting the most dangerous counterfeit products?**

My office cannot direct individual law enforcement operation priorities, but the Administration has undertaken several coordinated efforts to stop the entrance of counterfeit products into the stream of U.S. commerce through broad interagency collaboration. In deciding upon which problem areas to prioritize our resources, we consider a multitude of factors including employment effects, global competition, costs to the Federal government, how efficiently the Administration can pursue a solution, the burden on industry, and many others - but safety has always been paramount.

We are particularly concerned about unsafe products entering into the military or government supply chain. Recent reports issued by the Department of Commerce and the Government Accountability Office have found that counterfeits have infiltrated many sectors of the U.S. Government supply chain and have the potential to cause serious disruptions in national defense, critical infrastructure and other vital applications. In order to fight this problem we formed an interagency working group comprised of 14 U.S. Government components focused on eliminating counterfeit products from our supply chain. Law enforcement has stepped up efforts to investigate, arrest, and prosecute offenders who sell counterfeit goods to the military and U.S. Government. For instance, DOJ, the FBI, and ICE Homeland Security Investigations have investigated and prosecuted defendants under Operation Network Raider, which targeted the sale of counterfeit computer network hardware, including to the U.S. military. That Operation has led to more than 30 convictions and the seizure of more than \$143 million in counterfeit goods. Also, in June the IPR Center partners began Operation Chain Reaction to target counterfeits in the military and U.S. Government supply chain. In addition to the vanguard domestic and military investigative authorities, the IPR Center will be aided in its efforts to stop unsafe counterfeit products by the Consumer Product Safety Commission who joined as an IPR Center partner last year.

Ongoing efforts by the agencies to target the most dangerous counterfeit products have been successful. For example, CBP reported a 97 percent increase in seizures of safety-

relevant products at the border in FY 2010. Also, in September Operation Safe Summer, a two-month initiative involving several surge operations conducted by ICE, CBP, and the Mexican Tax Administration Service, targeted infringing imports of health and safety items at international mail and express carrier hubs in the United States and Mexico, leading to 800 seizures including counterfeit automobile airbags, rifle sites, cellular phones and chargers, and beauty products. Another similar international operation targeted towards safety-relevant products is slated for fall 2011. Recently, as we reported in our April/May/June 2011 *Spotlight*, the U.S. Government has had a recent string of successes in stopping or punishing infringement related to products that threaten health and safety including:

- An 87-month prison sentence was imposed on June 3 for trafficking in fake weight loss drugs; one of the victims of the fake drugs suffered a mild stroke.
- Also on June 3, a 48-month prison sentence was imposed on an operator of an Internet pharmacy which sold counterfeit and misbranded drugs to treat conditions including heart disease and psychiatric disorders. The defendant was apprehended in Costa Rica and extradited to the United States.
- On April 4, a 33-month prison sentence was imposed on a seller of counterfeit pills that contained a substance used in sheetrock manufacturing.
- On May 9, two 37-month prison sentences and one 30-month prison sentence were imposed on people engaged in selling hazardous counterfeit lead jewelry with over 20 times the lead deemed safe by the Consumer Products Safety Commission.
- Also, on May 9, a guilty plea from an individual for trafficking in over 2,000 counterfeit exercise equipment machines.
- A seizure of 30,000 counterfeit cans of sardines in June.
- On May 17, an indictment for selling 6,000 units of counterfeit diabetic test strips.

These examples are demonstrative of the efforts the Administration has taken and will continue to take to stop dangerous counterfeit products from harming consumers.



2. **You have hosted meetings with private companies, including Google, American Express, MasterCard, Visa, GoDaddy, and others, to take voluntary actions against illegal online pharmacies. In your testimony, you said that you have been encouraged by the willingness of private companies to collaborate to end the distribution of counterfeit pharmaceuticals online. Are there any companies we need to be pushing to step up and do more? What can we do to encourage this collaboration to continue?**

Our focus with the voluntary cooperation initiative is to help all relevant private sector actors to cooperate with each other to reach practical solutions that support public policy goals.

We have made significant progress combating fake online pharmacies by helping to facilitate a range of private sector actors - American Express, Discover, eNom, GoDaddy, Google, MasterCard, Microsoft, PayPal, Visa and Yahoo! - that are cooperating among themselves to battle a problem that poses an immense health and safety risk to the American public. Similar progress has been made with best practices recently developed by credit card companies and payment processors to withdraw payment processing services from sites selling counterfeit goods. In addition, on July 7, 2011, a collaborative agreement was announced between Internet Service Providers and content providers to combat online piracy. We would like to see similar progress with search engines and ad networks - both advertisers and ad brokers - to further disrupt the business model of illegal online sites that undermine U.S. businesses, U.S. job growth, and consumer confidence.

We believe that private sector cooperation is a positive step and consistent with our strategy of encouraging voluntary efforts to strengthen online intellectual property enforcement and with our broader Internet policy principles, emphasizing privacy, free speech, competition and due process. Congress can encourage the collaboration to continue by supporting the Administration's efforts and continuing to highlight the critical importance of intellectual property enforcement to our country, our economy and our citizens.

3. **In February 2011, Immigration and Customs Enforcement (ICE) seized mo00.com as part of a child pornography investigation. This seizure redirected more than 84,000 subdomains to a warning that mo00.com had been seized for involvement with child pornography, despite the fact that the overwhelming majority of these subdomains only had legal content. ICE fixed what they later admitted was an inadvertent mistake, but it took several days before the site was restored and the warnings were removed. Has your office considered putting out a set of best practices or guidelines that all law enforcement can rely on to conduct due diligence before seeking a court order to shut down entire top level domains?**

It is unfortunate that this happened. ICE realized there was a problem and moved quickly to correct it. Law enforcement's objective is only to go after serious criminal activity. There are significant safeguards in place in Operation In Our Sites to avoid mistakes, and ICE and DOJ are in the best position to address the operational specifics of those safeguards.

4. **China's piracy and counterfeit goods markets are notorious. What steps can we take to put more international pressure on China to reform its intellectual property infringement problems?**

In February 2011, USTR released the first stand-alone Notorious Markets List. The Notorious Markets List identifies over 30 Internet and physical markets worldwide that traffic in infringing products, including several markets in China. The list helps to raise public awareness of online piracy and counterfeiting, and encourages responsible governments to take increased enforcement action. The February 2011 Notorious Markets List has been followed by several notable actions involving listed markets in China and elsewhere. For example, *Taobao.com*, China's leading business-to-consumer website (and the fifth most-visited site in China), announced in response to having been listed in the Notorious Markets List, that it will launch a major campaign to stop online piracy and counterfeiting occurring on its site. In addition, the Government of Hong Kong took quick action against a market listed in the report, utilizing a new enforcement strategy, including increased patrols, arrests and prosecutions, and displaying an anti-piracy banner at the notorious "Ladies' Market." In July, Baidu, a leading Chinese search engine listed in the report, concluded a music licensing agreement with One-Stop China, a joint venture between the Universal Music Group, the Warner Music Group, and Sony BMG.

The United States has worked multilaterally with other trading partners to press China to do more to enforce intellectual property rights. For example, the Asia-Pacific Economic Cooperation (APEC)—which includes the United States, China, and 19 other members—will conduct a training workshop in September, during this year's third Senior Officials Meeting on investigating and prosecuting corruption and illicit trade, with a focus on counterfeit pharmaceuticals. On June 1, 2011, the APEC Mutual IPR Enforcement Operation, a joint operation between the United States and other APEC customs authorities, was initiated to target counterfeit pharmaceuticals and to develop model practices for intellectual property enforcement in international postal and express courier facilities. This is the first time a joint enforcement operation has ever been conducted under the auspices of APEC. China is an APEC member and it aspires to play a greater role on the world stage. Hence, the expectation that China will bring its intellectual property enforcement into conformity with international norms is even greater than it might otherwise be. For this reason, multilateral engagement through organizations like APEC will be an increasingly important means of applying international pressure on China to do more to enforce intellectual property rights. We will continue this multilateral approach, in addition to our bilateral engagement with China, going forward.

**During the hearing, you mentioned that the Trade-Related Aspects of Intellectual Property Rights (TRIPS) World Trade Organization (WTO) agreement was outdated and should be revised to reflect the enormous growth in intellectual property and new technologies since 1995, when TRIPS became effective. What changes would you recommend, and what other steps do you think we can take to address piracy via our trade agreements with China?**

The scope and scale of online intellectual property infringement that we currently face did not exist in 1995 when the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) entered into force, and as such, the TRIPS Agreement does not necessarily reflect many of today's enforcement challenges in the digital environment. Nonetheless, the TRIPS Agreement remains a vitally important minimum standard for intellectual property protection and enforcement. As a complement to the TRIPS Agreement, the United States has worked with many of our trading partners to address new challenges through dialogue, cooperation, and, where appropriate, through trade agreements. The Anti-Counterfeiting Trade Agreement (ACTA) is a prime example. ACTA provides a model for effectively combating global proliferation of commercial-scale counterfeiting and piracy in the 21st century through provisions that build on the minimum standards of TRIPS. It includes provisions on civil, criminal, border and digital environment enforcement measures, provisions on cooperation among ACTA parties to assist in their enforcement efforts, and provisions regarding best practices for effective intellectual property enforcement. ACTA negotiations were concluded last November with 37 other countries, who together with the United States represent over half of global trade. Although China was not a party to the negotiations, we are hopeful that as more countries sign ACTA, China will eventually join and implement this agreement.

With regard to addressing intellectual property violations via our existing trade agreements with China, the United States has previously pursued WTO disputes challenging China's intellectual property-related measures in cases where bilateral consultations with China were not successful. The United States will continue to vigilantly monitor China's implementation of TRIPS and other agreements and, where appropriate, seek recourse through WTO dispute settlement. However, short of filing cases in the WTO, the United States prefers to resolve issues with China through constructive bilateral engagement, including the following:

- China's Special IPR Campaign: Using the coordinated framework described in the IPEC Joint Strategic Plan section "*Enforcing our Rights Internationally*," we are working with the U.S. Trade Representative, other Federal agencies, and U.S. businesses to assess China's progress (and to encourage further action) under China's "Special Campaign Against Piracy and Counterfeiting," which China's

State Council launched in October 2010 and extended through the end of June 2011. We will continue to urge China, through trade dialogues such as the U.S.-China Joint Commission on Commerce and Trade (JCCT), to maintain a long-term, high-level focus on intellectual property enforcement and to continue its interagency coordination of IP enforcement at a senior political level, as they did during the Special IPR Campaign.

- Special 301 Report: This year, China was again listed on USTR's annual Special 301 Report as a Priority Watch List country. This list is reserved for countries with the most onerous or egregious acts, policies, or practices harming U.S. intellectual property owners. This year, in accordance with the IPEC Joint Strategic Plan action item "*Strengthen Special 301 Action Plans*," the USTR's Special 301 Report includes an open invitation to all trading partners listed in the report to cooperatively develop action plans to resolve IPR issues of concern. Agreement on such a plan will not by itself change a trading partner's status. However, in the past, successful completion of action plans has led to the removal of trading partners such as Saudi Arabia, Taiwan, and many others from Special 301 lists.
- Notorious Markets List: In February 2011, as part of the IPEC Joint Strategic Plan action item "*Identify Foreign Pirate Websites as Part of the Special 301 Process*," USTR released the first-ever out-of-cycle Notorious Markets List—a list of physical and online overseas markets that traffic in infringing products, including several markets in China. The list helps to raise public awareness of online piracy and counterfeiting and to focus our diplomatic efforts with China. For example, *Taobao.com*, China's leading business-to-consumer website (and the fifth most-visited site in China), announced in response to having been listed in the Notorious Markets List, that it will launch a major campaign to stop online piracy and counterfeiting occurring on its site. In addition, the Government of Hong Kong took quick action against a market listed in the report, utilizing a new enforcement strategy, including increased patrols, arrests and prosecutions, and displaying an anti-piracy banner, at the notorious "Ladies' Market." In July, Baidu, a leading Chinese search engine listed in the report, concluded a music licensing agreement with One-Stop China, a joint venture between the Universal Music Group, the Warner Music Group, and Sony BMG.
- Building Alliances with Chinese Law Enforcement: Ultimately, we need Chinese law enforcement to do more. Both the Attorney General and DHS ICE Director Morton have traveled to China to press their counterparts for increased cooperation to fight intellectual property crime. (This is the first time an ICE director has traveled to mainland China, and Director Morton made intellectual

property enforcement a major focus of his trip.) In addition, as part of the IPEC Joint Strategic Plan action item “*Enhance Foreign Law Enforcement Cooperation*,” we are working with foreign law enforcement to do more by having U.S. law enforcement on the ground working closely with Chinese law enforcement – building relationships that will lead to increased enforcement. To do so, we have been working with DOJ, FBI, and ICE to have IP-focused law enforcement personnel on the ground in China. In September 2010, the ICE Assistant Attaché in Guangzhou was designated as ICE’s first “IP Attaché” in China. The FBI is also preparing to send an IP-dedicated attaché to China later this year. In addition, the DOJ’s Criminal Division and the Chinese Ministry of Public Security (“MPS”) co-chaired the Intellectual Property Criminal Enforcement Working Group (“IPCEWG”) of the U.S.-China Joint Liaison Group for Law Enforcement Cooperation (“JLG”), which has resulted in an open dialogue on intellectual property criminal enforcement issues, increased information sharing on selected investigations, and a number of successful joint intellectual property operations.

- Software legalization: China recently made several commitments to ensure that its government agencies and State Owned Enterprises (SOEs) use only legitimate software. These commitments were achieved and are now being monitored under the IPEC Joint Strategic Plan action item “*Promote Enforcement of U.S. Intellectual Property Rights through Trade Policy Tools*.” For example, during the 21<sup>st</sup> JCCT in December 2010, China promised to allocate current and future budgets for purchasing, upgrading, and replacing agency software. At this meeting, China also announced that thirty SOEs will participate in a pilot project to encourage these SOEs to use only legitimate software. During President Hu Jintao’s state visit in January 2011, China committed to conduct audits to ensure that government agencies at all levels use legitimate software and to publish the auditing results as required by China’s law. We are now closely monitoring China’s efforts to ensure that these commitments are fully implemented and that its agencies and SOEs pay for the software they use.

RESPONSES OF VICTORIA ESPINEL, ALLEN GINA, AND ERIK BARNETT TO QUESTIONS  
SUBMITTED BY SENATOR GRASSLEY

**The Honorable Senator Chuck Grassley**  
**United States Senate Committee on the Judiciary**  
**Oversight of Intellectual Property Law Enforcement Efforts**

**1. In your opinion, what has been the most successful aspect of the PRO-IP Act in achieving its goals of comprehensive intellectual property rights enforcement?**

The creation of this office with its mission to coordinate enforcement across the agencies, coupled with strong support from the President, the Vice President and Federal agencies, as well as the bipartisan and bicameral support for our mission, has significantly increased the priority level placed on intellectual property enforcement.

We know that intellectual property enforcement is critical if we are to create and protect jobs, increase our exports, support our innovative industries and protect the safety of the public. Pursuing that objective has resulted in actions across a number of fronts. For instance, since 2010, law enforcement efforts have increased significantly, including both online enforcement through Operation in our Sites and physical enforcement. From fiscal year 2009 to 2010, ICE's opened intellectual property investigations were up more than 41 percent and arrests were up more than 37 percent, DHS intellectual property seizures were up more than 34 percent, and FBI intellectual property investigations opened were up more than 44 percent. In fiscal year 2010, CBP and ICE intellectual property seizures of consumer safety and critical technology increased by 97 percent. Outreach with rights holders and other stakeholders has significantly increased. The private sector has stepped up its efforts and expressed a willingness to do more to help U.S. businesses threatened by infringing activities by exploring voluntary actions aimed at reducing infringement. I believe that this is only the beginning. I will continue to work with Federal agencies, U.S. companies and other stakeholders to ensure that we are employing the most effective and coordinated actions to combat infringement.

**2. In your opinion, what is the greatest challenge that the IPEC faces with respect to IP theft?**

There are a number of challenges with enforcement against intellectual property infringement.

First, advancement in technology, particularly the critical role the Internet plays in our society and economy, has created a more complex environment for enforcement efforts. It is extremely important that our laws continue to keep pace with advances in technology to ensure that infringing activity, whether done physically or over the Internet, can continue to be addressed by our laws. Second, there is a substantial amount of infringement that originates beyond the jurisdictional reach of U.S. law. For example, sites engaged in infringement, including cyber-lockers - online file storage sites usually located in foreign countries - are a particular problem as they are capable of harboring massive amounts of digital content that is made available to infringers via peer-to-peer and similar networks. Third, piracy and the methods of infringers have become more sophisticated, further complicating the job of enforcement officials. Infringers have been using various methods to conceal their counterfeit goods including resorting to high volume, low value shipments sent via postal service or private courier to evade border enforcement. Fourth, the distribution chain for infringing goods is increasingly global in reach.

My office is acutely aware of these issues and we are engaged in coordinating an effective response with agencies that are responsible for enforcement.



**3. The PRO-IP Act increased penalties for certain intellectual property crimes. How effective have stricter penalties been in deterring intellectual property rights violations?**

Increased penalties for intellectual property crimes can effectively address the harm caused by these offenses and serve as a strong deterrent message to potential offenders. While the Prioritizing Resources and Organization for Intellectual Property Act's increase in penalties was helpful, more needs to be done to protect and grow American jobs and exports and to protect the health and safety of the American people.

In March of this year, we issued a White Paper that set forth the Administration's 20 legislative recommendations designed to strengthen intellectual property enforcement. These legislative recommendations seek to provide enhanced penalties for offenses involving the misappropriation of trade secrets, economic espionage, and for intellectual property offenses involving organized crime, repeat offenders, counterfeit drugs and sales of infringing products to the military and law enforcement. The recommendations also outline legislative changes that will provide enforcement agencies with additional tools to combat infringement and curb the sale of counterfeit pharmaceuticals. Finally, the White Paper recommends that Congress amend the laws to keep up with technology by making distribution by streaming or other new technology a felony similar to infringement by traditional distribution methods.

I look forward to working with Congress on these legislative proposals that seek to strengthen enforcement of U.S. intellectual property rights.

**4. What kinds of trends are you seeing with respect to intellectual property theft, piracy and counterfeiting? Are we able to keep up with the evolving methods and technologies utilized by IP criminals? Are the laws on the books able to keep up with the criminals?**

The trends that we are seeing with respect to intellectual property theft, piracy and counterfeiting include a substantial amount of infringement that originates in foreign countries that is beyond the jurisdictional reach of U.S. law. The Internet and other emerging technologies have provided unique challenges to law enforcement trying to enforce intellectual property rights. Intellectual property infringers have also developed more sophisticated methods using the latest technologies to attempt to avoid detection, further complicating the job of enforcement officials. Infringers have resorted to high volume, low value shipments sent via postal service or private courier to evade border enforcement. The global nature of distribution chain for infringing goods has further complicated efforts to enforce the intellectual property rights of U.S. rights holders.

However, we are making progress. For instance, from Fiscal Year 2009 to 2010, Immigration and Customs Enforcement intellectual property investigations are up more than 41 percent and arrests are up more than 37 percent, Department of Homeland Security intellectual property seizures are up more than 34 percent, and FBI intellectual property investigations are up more than 44 percent.

We will not solve the intellectual property theft problem by simply doing more of the same thing. Improved coordination, greater focus on enforcement and ensuring that our laws are strong are potential tools to address intellectual property infringement. The Joint Strategic Plan on Intellectual Property Enforcement seeks to advance many of those changes and we are implementing those changes. We have also adopted a new and innovative approach to combat infringement online, which focuses on increased law enforcement action, voluntary private sector cooperation, and increased education to the public about the risks of and damage done by infringement.

As to the effectiveness of the laws currently on the books, in March of this year, we issued a White Paper that set forth the Administration's 20 legislative recommendations designed to strengthen intellectual property enforcement. These legislative recommendations seek to provide enhanced penalties for offenses involving the misappropriation of trade secrets, economic espionage, and for intellectual property offenses involving organized crime, repeat offenders, counterfeit drugs, and sales of infringing products to the military and law enforcement. The recommendations also outline legislative changes that will provide enforcement agencies the tools to combat infringement and curb the sale of counterfeit pharmaceuticals. Finally, the White Paper recommends that Congress amend the laws to continue to keep up with technology by clarifying that distribution by streaming or other new technology is a felony, similar to infringement by traditional distribution methods. Throughout this legislative session,

Congress has acted on many of the recommendations including introducing bills to punish economic espionage, fight counterfeit drugs, clarify that commercial streaming is a felony, improve disclosure authority, and increase penalties for sales of counterfeits to the military. I look forward to working with Congress on these legislative proposals that seek to strengthen enforcement of U.S. intellectual property rights.

**5. In your opinion, in what ways has the increased FBI-DOJ partnership been productive? How can it be improved in the future?**

Our Strategy committed to ensure the efficiency and coordination of Government resources in intellectual property rights enforcement, including the coordination of Federal, state, and local law enforcement. In February 2010, U.S. Attorney General Eric Holder announced the formation of a Department of Justice Task Force on Intellectual Property, which, among other things, prioritized coordinating with state and local law enforcement partners as a way to strengthen efforts to fight intellectual property crimes. Consistent with this priority, the FBI has increased its coordination with state and local law enforcement. For example, the FBI in California worked with the Placer County Sheriff's Office and Galt Police Departments on an investigation that led to the arrest and subsequent conviction of a defendant trafficking in a range of counterfeit items with an estimated retail value of over \$7 million, including some counterfeit goods bearing the "UL" safety mark. In November, the defendant was sentenced to 26 months in prison, and was ordered to pay a \$25,000 fine and \$9,575 in restitution. Also, the multitude of investigative efforts that FBI agents put forward build the solid cases the DOJ U.S. Attorney's Offices need for convictions and stiff penalties for intellectual property criminals.

**6. What are your thoughts on how the various enforcement agencies are cooperating in the federal government's efforts to combat intellectual property theft? What can be improved?**

The coordination and the response among the various enforcement agencies have been good. The Joint Strategic Plan on Intellectual Property Enforcement (Strategy) that we issued in June 2010 reflected the cooperative efforts of the Federal agencies, and the progress reflected in the report to Congress that my office released in February and the Anniversary report we released in June, are a good indication of our effective coordination and ongoing cooperative work to implement that Strategy. My office coordinates through a variety of formal and informal means, including daily correspondence and regular calls with the enforcement agencies as well as more formal interagency meetings. With the passage of the Prioritizing Resources and Organization for Intellectual Property Act of 2008, Congress created an interagency intellectual property enforcement advisory committee, which has been helpful in coordinating these efforts. Furthermore, on February 8, President Obama signed Executive Order 13565 establishing a Cabinet-level advisory committee, chaired by IPEC, comprised of the heads of the departments responsible for intellectual property enforcement.

A key tool that highlights agency cooperation has been the establishment of four interagency working groups concerning U.S. Government procurement, U.S. Government personnel stationed overseas, international training efforts, and counterfeit pharmaceuticals. These working groups have used a collaborative approach to tackling enforcement issues identified in the June 2010 Joint Strategic Plan on Intellectual Property Enforcement that has increased the amount and quality of coordination between the agencies. For example:

- The procurement working group is made up of 14 government components and is charged with developing legislative, regulatory and policy recommendations for President Obama to eliminate counterfeit products in the U.S. Government supply chain.
- The overseas personnel working group identified 17 countries as priority countries for intellectual property enforcement and recommended that U.S. embassies in each of those countries establish senior-level interagency working groups. The working groups have now been established and each working group has completed detailed work plans setting out the actions that embassy personnel will take to address the specific challenges in each country.
- The international training working group was formed to improve interagency coordination of international capacity building and training. As a result of this group's work, in March, the USPTO launched a publicly-accessible, online database that will lead to more efficient use of resources by allowing different agencies to share materials and avoid duplicative work.

- Last March, the counterfeit pharmaceutical working group presented a strategy to the Vice-President and to Congress that detailed how the U.S. Government would fight counterfeit drugs including from illegal online pharmacies. The group is now working on implementation of that strategy.

The IPR Center, hosted by ICE, is an excellent example of regulatory agencies and law enforcement bodies coordinating together to use the expertise of its member agencies to share information, develop initiatives, coordinate enforcement actions, and conduct investigations related to intellectual property theft. The FBI and IPR Center partners have improved the coordination of intelligence of global intellectual property threats by examining, reporting and sharing intelligence on those threats. The IPR Center has also been making sure resources do not overlap by working with IPR Center partners to de-conflict investigative activity. The de-confliction process has been collaborative and complementary, using each agency's comparative advantage to most efficiently conduct the investigation. These various agencies have cooperatively worked on investigations by using their agency-specific expertise to develop cases with one another. This includes FDA pharmaceutical testing, CPSC product safety analysis, IRS financial audits, Postal Service package inspections, CBP import targeting, ICE undercover operations and many other activities.

Federal, state and local law enforcement have teamed up to combat intellectual property crimes throughout the country as evidenced by the 26 ICE-lead Intellectual Property Theft Enforcement Teams (IPTETs) and the 4 FBI-lead Intellectual Property Task Forces, and their results have been telling. For example, the Houston IPTET had three significant enforcement actions over a four-month period. In July, it seized nearly a half million dollars' worth of counterfeit goods at a local boutique; in September, it seized more than \$1 million of pirated DVDs at a local flea market; and, in October, it seized \$2.5 million of counterfeit goods at three local businesses. Also, the FBI in California worked with the Placer County Sheriff's Office and Galt Police Departments to investigate and arrest a trafficker of counterfeit items – including some bearing the “UL” safety mark – that, if genuine, would have been worth over \$7 million. In November, after being found guilty, the trafficker was sentenced to 26 months in prison, and was ordered to pay a \$25,000 fine and \$9,575 in restitution.

Federal, state and local authority coordination has also had positive effects beyond our borders as various agencies demonstrated in February with the extradition from Paraguay of a fugitive who allegedly supported the terrorist group Hezbollah with profits from counterfeit goods. A wide range of federal, state, and local law enforcement agencies coordinated on that case including the FBI, ICE, Homeland Security Investigations (HSI), the New Jersey State Police, the Internal Revenue Service, the U.S. Secret Service,

Defense Criminal Investigative Services, the Department of Commerce, the U.S. State Department, U.S. Customs and Border Protection (CBP), the Bureau of Alcohol, Tobacco, and Firearms and Explosives, Federal Air Marshals, Pennsylvania State Police, and the Philadelphia Police Department.

With respect to improvements, there is a tremendous problem involving the export of illegal or otherwise inadmissible pharmaceuticals that FDA cannot destroy. CBP and FDA are working to address this matter and my office has consistently been engaging both agencies and other stakeholders – both public and private – on how best to proceed. Going forward, we expect to be able to put the complexities of this issue into context and to propose a way to address it in the update to our pharmaceutical strategy, which we plan to release this fall.

## RESPONSES OF GORDON SNOW TO QUESTIONS SUBMITTED BY SENATOR GRASSLEY

**Responses of the Federal Bureau of Investigation  
to Questions for the Record  
Arising from the June 22, 2011, Hearing Before the  
Senate Committee on the Judiciary  
Regarding Oversight of Intellectual Property Law Enforcement Efforts**

**Questions Posed by Senator Grassley**

- 1. In your opinion, what has been the most successful aspect of the PRO-IP Act in achieving its goals of comprehensive intellectual property rights enforcement?**

**Response:**

The Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act) has enabled the FBI to build a robust and effective intellectual property (IP) enforcement program that focuses on the most significant threats to U.S. economic and national security interests. The funding made available by the PRO-IP Act has enabled the FBI to dedicate approximately 51 Special Agents to intellectual property rights (IPR) and to establish an FBI unit dedicated to IPR. The physical placement of the IPR unit in the National IPR Coordination Center (hereafter IPR Center) has been particularly helpful, fostering increased collaboration among the represented agencies. The IPR unit manages several aspects of the FBI's response to IPR challenges, including case initiation and investigation, case management, training and outreach, intelligence fusion, research, and other tactical and strategic initiatives. The IPR unit also addresses international and complex IPR matters and deploys to FBI field offices as needed to assist in IPR cases.

- 2. In your opinion, what is the greatest challenge that the FBI faces with respect to IP enforcement? What is the greatest challenge that we face with respect to IP theft?**

**Response:**

The greatest challenges in IPR enforcement arise from the fact that IP crime takes place in the global economic market and, therefore, addressing it requires coordination with international partners. Countries place different priorities on IPR enforcement because their laws differ and the impact of IPR violations is not

---

*These responses are current as of 9/15/11*



uniform from country to country. For example, infringements that are considered high priority in one country or region may not be viewed as serious in another country or region.

The most significant challenges with respect to IP theft, which are predictably related to these law enforcement challenges, include the role played by international organized crime, the large-scale data breaches that can threaten U.S. economic security, and online fraud.

**3. The PRO-IP Act increased penalties for certain intellectual property crimes. How effective have stricter penalties been in deterring intellectual property rights violations?**

**Response:**

We are not aware of existing metrics for quantifying the impact of increased penalties on the incidence of criminal activity, and it is always difficult to determine what factors have led to both increases and decreases in crime. This is particularly true in the IPR arena, where the scope and nature of a given type of crime can change rapidly along with changes in technology and other factors. So, even if one factor, such as stricter penalties, may serve as an effective deterrent, other factors may exert even greater influence.

**4. Are there any additional tools that you'd like to see enacted into law that would assist you in your efforts to protect intellectual property rights, both here and abroad?**

**Response:**

The FBI's ability to investigate and counter IPR violations could be bolstered through a range of legislative provisions. These recommendations are described in detail in the "Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations," released in March 2011 and available online. Among these recommendations are the following:

We believe the integrity of the sentencing structure is enhanced when we address serious crimes with serious punishments. For example, economic espionage is one of the most serious IP violations, but violators face a statutory maximum sentence of just 15 years in prison. In addition, given the importance of protecting the public from the risks associated with counterfeit pharmaceuticals and medical devices, cooperation from importers and manufacturers is essential. To obtain this cooperation, the White Paper recommends legislation requiring that

those entities notify the Food and Drug Administration and other relevant agencies when they discover counterfeit drugs or medical products.

Finally, the White Paper recommends extending wiretap authority to criminal copyright and trademark offenses subject to the existing legal protections that apply to wiretaps for other types of crimes. This authority would enhance our ability to effectively investigate those offenses, including by targeting organized crime and the leaders and organizers of criminal enterprises.

**5. The federal government has a finite number of resources to conduct its law enforcement investigations and prosecutions. Yet piracy and counterfeiting are surging all over the world, as well as online. Do you think that rights holder actions can alleviate some of the burdens on federal law enforcement and effectively combat IP theft?**

**Response:**

Rights holders who have the knowledge and ability to detect, prevent, and protect against IP crimes could alleviate some of the burdens on federal law enforcement, while those who lack the necessary experience or resources will continue to seek law enforcement assistance. Many of the criminals and criminal organizations that routinely profit from IP violations are so broadly based or sophisticated that they cannot be significantly affected by the efforts of individual rights holders. In these cases, and when these organizations are involved in other criminal activity, such as drug trafficking, forced labor, and fraud, federal law enforcement involvement may be needed to fully and safely investigate and prosecute the IP crimes.

**6. What kinds of trends are you seeing with respect to intellectual property theft, piracy and counterfeiting? Are we able to keep up with the evolving methods and technologies utilized by IP criminals? Are the laws on the books able to keep up with the criminals?**

**Response:**

As IP criminals become more sophisticated, they are increasingly using the Internet to conduct their activities and the types of IP violations are becoming more varied. While FBI investigators have the technical ability to address high-tech crimes, this work can be labor intensive. In addition, the Internet allows criminals to commit extremely high numbers of these crimes, and the volume of the resulting forensic work poses significant law enforcement challenges. The issues currently being addressed include:

---

*These responses are current as of 9/13/11*

Digital Piracy through Online Channels. The Internet permits the immediate digital distribution of pirated media content through “streaming.” Many of the illegal audio and video streaming sites operate overseas to avoid U.S. law enforcement efforts and are highly profitable, bringing in millions of dollars in subscription fees and advertisement revenues, while providing no compensation to the owners of the copyrighted content being pirated. The Administration has proposed updating the law to make clear that, in appropriate cases, infringement by streaming is a felony.

Greater Complexity of Counterfeit Products. As manufacturing and supply chains become global and decentralized, the types of products being counterfeited, the materials supporting counterfeiting enterprises, and the techniques used to counterfeit are all becoming more advanced. Consumer goods such as purses and shoes are no longer the primary counterfeit products. Instead, products such as circuit breakers, integrated circuits, automotive components, and defense industry components must be scrutinized, since all can be counterfeited and some may pose a great hazard to both national security and individual consumers. Even this scrutiny has become more challenging, because it is becoming more difficult to distinguish counterfeits from authentic goods without conducting appropriate tests, such as the x-raying of computer chips.

Supply Chain Vulnerabilities. Counterfeiters are actively seeking opportunities to exploit supply chain vulnerabilities, divert supplies, and evade measures designed to ensure supply chain integrity. For example, some counterfeiters engage in “cyber-squatting,” where illegitimate sellers operate seemingly official web sites, connecting unsuspecting consumers to counterfeit goods.

U.S. Fabrication of Infringing Goods. While a majority of the infringing goods are manufactured in other countries, manufactured generic goods may be shipped to the United States in parts and then fabricated here to circumvent legal constraints. For example, thousands of unmarked shirts might arrive in the United States in one package with counterfeit labels and infringing embroidery being applied thereafter.

Changing Importation Methods. The methods by which counterfeit goods are imported into the United States are changing, with products being routed through numerous countries before arrival here in order to disguise their countries of origin. This trans-shipping and drop-shipping misleads customs inspectors, impeding detection and enforcement efforts. Criminals are also dividing bulk

shipments into multiple packages and sending them through smaller shippers and express mail services (such as FedEx and UPS) in order to avoid detection by customs inspectors.

Increased Challenges to Consumer Awareness. Although counterfeit goods were formerly sold in “secondary” or “aftermarket” venues, where customers knew they were purchasing infringing goods, they are increasingly being sold in the “primary” market, where the vendors and products appear to consumers to be legitimate. One alarming example of this shift is in the counterfeit pharmaceutical market, where the apparent authenticity of the medical products being sold can pose a serious threat to the public’s health and safety.

Broader Participation in IP Crime. The enterprises involved in IP crime have become more diverse, with participants now including individuals, gangs, and organized crime syndicates. In addition to the diversity of the participants, the scale and scope of infringements have also become more varied. Investigators encounter both organized networks distributing pirated media at flea markets and individuals stealing trade secrets valued in the hundreds of millions of dollars.

**7. What are the FBI’s particular priorities with regard to intellectual property enforcement?**

**Response:**

The FBI’s highest priorities with respect to IP enforcement are to disrupt and dismantle international and domestic manufacturers and distributors engaged in IP crimes that pose immediate threats to health and safety, have a national security nexus, involve organized crime, or may exert significant economic impact.

**8. FBI’s new Intellectual Property Rights Unit is located at the IPR Center, and the FBI has been a partner of the IPR Center for over a year now. In what areas has the FBI’s partnership with the IPR Center been most effective, and where can it improved?**

**Response:**

As noted in response to Question 1, above, the physical placement of the IPR unit in the IPR Center has fostered increased collaboration among the represented agencies, allowing us to interact with our counterparts daily and engage in early coordination of investigations in which we have mutual interest. Although internal FBI network security restrictions currently require separation of the IPR

---

*These responses are current as of 9/13/11*

Unit from the rest of the IPR Center, we are seeking solutions that will permit a more open workspace, further enhancing and strengthening our partnership with other IPR Center agencies. Even with that impediment, though, there are significant benefits inherent in the collaboration facilitated by the Center, including the following.

- Frequent meetings allow participating agencies to chart the Center's strategic direction, discuss recently initiated investigations, review databases for any investigative overlap, initiate joint agency investigations when appropriate, and take other measures to streamline the investigative process and minimize reliance on limited resources.
- The FBI and the Center's Outreach and Training Unit coordinate their training and outreach closely to avoid a duplication of efforts, to enhance efficiency, and to ensure that we provide consistent messages. This coordination also allows us to ensure the proper staffing of training and outreach efforts and to make efficient use of the FBI's provision of instructors and travel funds to assist the Center's IPR training efforts.
- The FBI has established an Intelligence Fusion Group at the Center, the mission of which includes defining the IPR threat picture, sharing strategic intelligence, establishing joint collection requirements, and producing joint intelligence products.

**9. Since the PRO IP Act, the FBI has hired 51 new IP-dedicated agents, most of which are supporting the Department of Justice's CHIP units. How effective has this partnership been? What has been done to ensure that the new agents are effectively supporting CHIP investigations?**

**Response:**

The FBI's IP agents have been strategically assigned. While some of these agents have been assigned to the IPR Center, as discussed above, most are aligned with the Department of Justice (DOJ) Computer Hacking and Intellectual Property (CHIP) program. The CHIP program consists of over 200 Assistant United States Attorneys (AUSAs) specially trained to prosecute cyber crime and intellectual property cases. These AUSAs work closely with DOJ's Computer Crime and Intellectual Property Section (CCIPS), which has primary responsibility for developing DOJ's computer and intellectual property offense enforcement strategies, providing programmatic support to the CHIP network, and

---

*These responses are current as of 9/15/11*

coordinating computer crime and intellectual property investigations and cases that may significantly impact more than one district and/or other countries.

In 2010, 20 FBI agents joined the 31 agents who were then devoted to investigating IP crimes, bringing the number of dedicated IP agents to 51. The 20 newly assigned agents are deployed to locations around the country where IP crimes are of particular concern, working with both CHIP AUSAs and CCIPS to help coordinate complex investigations, develop investigation and prosecution strategies, and coordinate multi-district cases. We believe these agents have significantly strengthened the FBI's ability to investigate IPR violations through their partnership with CHIP AUSAs and their close coordination with our state and local law enforcement partners and our international counterparts.

**10. What types of IP investigations are these agents' highest priorities, and what are their criteria for deciding which investigations to pursue?**

**Response:**

The highest priorities for the IP agents supporting CHIP AUSAs are the same as the highest priorities for IP agents, generally: IP crimes that pose immediate threats to health and safety, have a national security nexus, involve organized crime, or may exert significant economic impact. Even within these top priorities, though, the determinations of which investigations to pursue, what resources to allocate, and what priority to assign depend upon the unique facts of each case, and these facts can change during the course of an investigation. For example, while immediate threats to health and safety clearly receive a very high priority, those threats may only become evident, or may be refuted, during the course of a broader IP investigation, raising or lowering the priority of that investigation as the investigation evolves. In cases of monetary loss, factors affecting an investigation's priority might include the amount of the loss and the degree to which other remedies are available to the victim rights holder.

**Questions Posed by Senator Coburn**

**11. According to your 2009 and 2010 Annual Reports required by the PRO-IP Act, the FBI has used funding authorized by that Act to hire 51 new agents to work on IP enforcement-related cases. According to the PRO-IP Act, these agents are supposed to be used for the investigation and coordination of intellectual property crimes. Do any of those agents spend time NOT working on IP cases? Why?**

---

*These responses are current as of 6/13/11*

**Response:**

As noted above, the PRO-IP Act has enabled the FBI to dedicate approximately 51 Special Agents to IPR, with 20 additional agents joining the 31 agents already devoted to IP crimes in 2010. The appropriations included in the PRO-IP Act have enabled the FBI to place IP-dedicated Special Agents at the IPR Center and in 21 of the FBI's 56 field offices. In fact, by using funds provided by the PRO-IP Act along with other appropriations, we have been able to increase the amount of time Special Agents dedicate to the investigation of IP crime so that these resources now exceed the 51 Special Agents called for in the PRO-IP Act.

In addition to investigating IPR crimes, Special Agents dedicated to IPR develop and implement strategic investigative initiatives and work with local law enforcement authorities and industry partners in support of IP investigations. They also attend and provide IPR training and continue their career-path training. Although these IP agents occasionally support other high-priority matters in their field offices, this other activity is more than offset by the resources provided outside the PRO-IP Act and used to work IP cases in the 35 FBI field offices for which no PRO-IP Act agents were allocated. These resources are also supplemented by those used to investigate economic espionage violations under 18 U.S.C. § 1831; these violations are assigned to national security units, which are resourced separately from, and in addition to, the approximately 51 agents working other IPR violations.

**12. In 2009, FBI received \$9.4 million to hire 31 agents. \$8 million was for salaries for 31 agents and 15 support personnel, and \$1.4 million was for other funding, which included \$331,000 for travel and training of the new agents. The salary expenses are an average of approximately \$174,000 in salary per person (agents and support personnel) and \$10,677 in travel expenses per agent.**

**a. Is \$174,000 the average salary for support personnel and/or an agent? If not, what is average salary for FBI support personnel? What is the average salary for an FBI agent?**

**Response:**

In Fiscal Year (FY) 2011, the average annual compensation (including salary, benefits, locality pay, and, for Special Agents, availability pay) for an FBI Special Agent is \$171,000 and for a professional support employee is \$89,000. The FBI

---

*These responses are current as of 9/13/11*

does not, though, use average compensation when requesting new positions. Instead, we use a cost module for new positions that was developed in collaboration with DOJ and the Office of Management and Budget and that includes compensation and other costs associated with hiring and supporting new employees (this includes, for example, the costs of the background investigations of these new employees and of their initial supplies, including computers).

Following are the costs used in the FY 2009 IPR enhancement referenced in the question.

Type of Position	Number of Positions	FY 2009 Cost Module Funding Per Position*	Total Personnel Cost
Special Agent	31	\$215,000	\$6,665,000
Clerical	9	\$70,000	\$630,000
Investigative Support	6	\$113,000	\$678,000
<b>TOTAL</b>	<b>46</b>		<b>\$7,973,000</b>

\*Note: The "Cost Module Funding Per Position" includes half of the first year's compensation and the non-personnel costs (developed in the cost module) required to hire a new employee.

**b. Why was \$10,000 spent on each agent for travel? Does this amount include conferences? If so, please break down the 2009 and 2010 travel expenses to show use of the funds.**

**Response:**

As reported by the FBI in the 2009 PRO-IP Act Annual Report to Congress, the FBI received \$8 million to support the IPR program for FY 2009. Personnel funding of \$6.580 million enabled us to place 26 specially trained Agents in the field and 5 Agents in the FBI Headquarters (FBIHQ) IPR Unit located at the IPR Center. Non-personnel funding, in the amount of \$1.420 million, included \$1.009 million to be used for equipment and supplies in the field and equipment and construction costs for the FBIHQ IPR Unit. The remaining amount of \$331,000 was used to fund the following.

---

*These responses are current as of 9-13-11*



- Approximately \$60,000 funded training and travel for personnel assigned to DOJ's CCIPS.
- Approximately \$62,000 funded training and travel costs for FBI Agents, including newly designated IPR Agents, and Intelligence Analysts who work IPR matters, including their attendance at a comprehensive 3-day IPR training conference in California.
- Approximately \$209,000 funded domestic and international IPR operational travel and training costs, including the attendance of more than 20 FBI employees at the 2009 INTERPOL International Law Enforcement IP Crime Conference in Dublin, Ireland. This conference, which is focused solely on operational activities, brings law enforcement organizations, regulatory agencies, private sector IP crime investigators, and prosecutors together to develop practical operational responses to IP crimes. The FBI both contributes to this conference and benefits from attending it. We contribute by providing all translation services, making a targeted address to the conference as a whole, and leading several breakout sessions. We benefit because the conference allows us to: develop new relationships and enhance existing relationships with the law enforcement agencies of other countries responsible for responding to IPR issues; share trends and intelligence in regional and global IP crime; facilitate case referrals and lead generation and response; share best practices in IP enforcement efforts; and develop protocols for joint/cooperative responses to global IPR matters. Although we can discuss them only in a classified setting, our attendance has directly resulted in investigative leads, case referrals, and international assistance in IPR investigations, and INTERPOL has recently moved to adopt a Theft of Trade Secrets program.

**13. How did the FBI decide where to place the 51 additional agents it has hired over the past two years? Have those agents made an impact on the number of cases opened, investigated and concluded? Why or why not?**

**Response:**

As noted above, in 2010 20 FBI agents joined the 31 agents who were then devoted to investigating IP crimes, bringing the number of dedicated IP agents to 51. In FY 2010 the FBI conducted an extensive strategic review of the IPR program, including the threat information provided by our partners in industry

associations, international and domestic law enforcement organizations, and the intelligence community. In addition, the FBI analyzed its pending cases to determine whether the most significant threats were being addressed. Based upon that review and analysis, dedicated IP agents were assigned to 22 of DOJ's 25 CHIP units and FBI IP Coordinators were assigned to the remaining three units.

While this placement of IP agents has increased the number of newly initiated cases (particularly the numbers of trade secret investigations and health and safety investigations), we believe the more significant impact has been the increase in the significance, complexity, and scope of the IP cases we are able to investigate successfully. The addition of IP agents and their placement with CHIP units have improved our ability to address the increasingly complex IP threat, which includes both domestic and international elements.

(The following questions were posed to all witnesses - the FBI is responding solely for the FBI)

**14. Could you each explain briefly your responsibilities in IP enforcement and how you coordinate with one another?**

**Response:**

Because of the FBI's dual responsibilities in intelligence and law enforcement, we are ideally positioned to examine the organizations and individuals involved in IP theft. The FBI's strategic objective is to disrupt and dismantle international and domestic manufacturers, distributors, and criminal organizations engaged in IP crimes, focusing in particular on the thefts of trade secrets and the sales of counterfeit goods that threaten health and safety and on copyright and trademark infringements that involve national security, organized crime, or significant economic interests.

As discussed further below, the IPR Center is critical to the effective coordination of these complex investigations. While investigators at the FBI and other agencies coordinate directly with DOJ prosecutors in individual cases, and planning and consultation between agencies can efficiently address short-term or narrow-scope issues, strategic and policy coordination and deconfliction benefit from the ongoing interaction among the agencies participating in the IPR Center.

**15. How effective has the IPR Center been at coordinating agency efforts and de-conflicting cases to ensure no duplication occurs?**

---

*These responses are current as of 9/13/11*

**Response:**

The IPR Center has become an invaluable tool for coordinating large initiatives, collaborating on pending matters, and reducing the risk that simultaneous or overlapping investigations will jeopardize the work of one of the investigating agencies. During weekly meetings managed by U.S. Immigration and Customs Enforcement, partner agencies discuss recently initiated investigations and are tasked with querying their databases to identify any investigative overlap. This coordination ensures the effective use of limited resources, allows for the deconfliction of incoming leads, and presents opportunities to initiate joint agency investigations. In addition, the IPR Center's Intelligence Fusion Group allows the FBI and its partner agencies to obtain a clear picture of the IPR threat, share strategic intelligence, establish joint collection requirements, and produce joint intelligence products.

**16. How does each of your agencies coordinate with private industry to improve your enforcement efforts?**

**Response:**

The FBI and our IPR Center partners use executive meetings, awareness programs, conference participation, and targeted training opportunities to coordinate with private industry to improve IPR enforcement. In our efforts to develop and maintain close working relationships with domestic and international industry partners, the FBI focuses, in particular, on "subject matter expert" learning exchanges, investigative referrals, and joint case initiatives. For example, in Los Angeles the inclusion of private sector brand (or rights) holders, subject matter experts, prosecutors, and law enforcement agencies in an Intellectual Property Loss Mitigation Working Group has made this an excellent forum for the exchange of information. The FBI has also hosted a small working group of corporate security officers from Fortune 100 companies with a view toward improving the sharing of IP theft information and strengthening relationships between law enforcement agencies and industry. When IPR Center researchers were recently preparing a comprehensive threat report, industry partners collaborated in the effort, providing valuable insight into the IP threats facing various industries, including the automotive, aircraft, media content (software, music, and movies), luxury goods, and pharmaceutical industries.

**17. How has the private industry stepped up their efforts to enforce their rights and coordinate with the federal government?**

---

*These responses are current as of 9/15/11*

**Response:**

The FBI and our IPR Center partners meet frequently with industry representatives to share information regarding the IP threat. Training programs conducted by DOJ and the State Department for foreign industry representatives often include a full day on which industry representatives discuss the identification of counterfeits and develop effective working relationships with law enforcement agencies. As a result of the IPR Center's domestic and international training and outreach, a number of key industries are building critical awareness of piracy and counterfeiting issues.

To successfully investigate IP crimes, the FBI and partner agencies often rely on referrals from the victims of infringement and work closely with industry experts to distinguish counterfeit and pirated goods from legitimate items. Increasingly, industry officials are proactively stepping forward to collaborate with the FBI regarding data protection and the theft of trade secrets.

**18. How much does each of your agencies spend annually on IP enforcement? Has that increased since the passage of the PRO-IP Act in 2008?**

**Response:**

The FBI has increased the resources dedicated to IPR since the 2008 passage of the PRO-IP Act. Prior to FY 2009, the FBI did not have a dedicated IPR budget, instead supporting its IPR activities with base funds. The appropriation of IPR-specific resources in both FY 2009 and FY 2010 provided dedicated personnel and non-personnel IPR resources. The FBI spent approximately \$7.5 million in FY 2009 and approximately \$14.4 million in FY 2010 on IPR matters. In FY 2011, the FBI anticipates spending approximately \$14.1 million on IPR efforts. FY 2010 funding is greater than FY 2011 funding because FY 2010 funding includes the first-year cost module funding necessary to establish the newly authorized positions (including background checks and supplies, such as computers), and this funding is not necessary in full after the first year.

**19. Has the amount and/or quality of agency coordination improved since the formation of the Office of the IP Enforcement Coordinator in 2009? Why or why not?**

**Response:**


---

*This response is unclassified.*

Several areas of inter-agency coordination have improved since the formation of the Office of the IP Enforcement Coordinator (IPEC), including joint investigations and strategic planning, coordination with international partners, and the effectiveness of working groups. For example, the Office of the IPEC spearheaded inter-agency efforts to address the online sale of counterfeit pharmaceuticals and the presence of counterfeits in the government supply chain, coordinated the development of legislative proposals on behalf of the Administration with input from all affected agencies, and assisted in coordinating training and capacity building programs to increase awareness and minimize duplication of these programs.

**20. Are there certain products or offenses that dominate your enforcement efforts?**

**Response:**

The FBI's IP-related strategic objective is to identify and dismantle international and domestic manufacturers, distributors, and criminal organizations engaged in IP crimes, focusing on those thefts of trade secrets and distributions of counterfeit goods that pose a threat to health or safety and those copyright and trademark infringement cases with a national security, organized crime, or significant economic impact.

The following types of cases have necessitated increased law enforcement efforts:

Complex Thefts of Trade Secrets. Technological advancements have greatly affected both the significance of trade secret violations and the complexity of the related investigations. The types of trade secret cases being investigated when the Economic Espionage Act was passed in 1996 are now rare. In the past, an employee simply copied a sales list or a set of blueprints and attempted to sell it to a competitor. Investigators often located the physical evidence of these crimes and, on occasion, the FBI was alerted by the competitor and was able to catch the perpetrator in the act by setting up an undercover purchase. These efforts often resulted in irrefutable evidence that frequently led to guilty pleas. Now, an insider downloads gigabytes of information from the computer of a victim rights holder and transmits it instantaneously to a competitor or hostile entity. In these cases, it is very difficult to locate evidence and to prove some elements of the crime, such as intent. The average time spent on such investigations has increased substantially.

Counterfeit Pharmaceuticals and Other Goods that Threaten Health and Safety.

The counterfeit arena is no longer dominated only by luxury goods and clothing, nor is it confined to the “secondary market,” in which consumers seek out and deliberately purchase less expensive copies of name brand items. A growing concern is the trend toward potentially dangerous “primary market” counterfeits, including aircraft and auto parts, electrical components and appliances, and pharmaceuticals. Substandard product knock-offs may find their way into the legitimate supply chain and are often purchased in the belief that they are genuine, posing a significant risk to safety and health. For example, counterfeit pharmaceuticals may contain harmful substances, excessive amounts of active ingredients, little or no active ingredient, or even substitute types of active ingredients used in other pharmaceuticals, all of which may be dangerous to the consumer.

Copyright Infringement Committed Online. Online piracy dominates copyright infringement, whether through peer-to-peer (P2P) file-sharing, web sites offering downloadable pirated content, or online stores and auction sites where pirated movies and software can be purchased on disc. These methods have overtaken traditional avenues of copyright infringement, including the sale of pirated compact disks, DVDs, software, and books through storefronts and flea markets. Though the piracy of discs and other media is still widespread, online piracy accounts for an increasing proportion of the copyright infringement activity and its enforcement will be reflected in a larger proportion of our investigative efforts.

Streaming. A more recent development in online copyright piracy is the growth in the “streaming” of pirated audio and video content, which can be accomplished without downloading a complete copy. In the past, the costs of the bandwidth and the equipment necessary to stream content, particularly video content, have discouraged this abuse. Decreasing costs, the deployment of broadband to consumers, and the ability of providers to recoup costs through online advertising networks have made streaming a viable option for a growing number of content providers, both legitimate and illegitimate. A number of large-scale pirate sites now deliver infringing content through streaming, often from overseas to avoid U.S. enforcement efforts, and many bring in millions of dollars in subscription fees and advertising revenue for their owners, while providing no compensation to the owners of the pirated content.

**21. Are there certain countries that pose more serious threats to American intellectual property than others?**

**Response:**

The threat to our intellectual property is diverse in nature and global in reach. Although no one country stands alone as the cause of intellectual property crime, China is a significant source of both counterfeit and pirated products imported into the United States and the theft of trade secrets. For example, of the eight indictments under the economic espionage statute (18 U.S.C. § 1831) since it was passed in 1996, six had a nexus to China.

**22. Why kind of discussions have you been having with China?****Response:**

The FBI's Legal Attaché in Beijing routinely engages with Chinese officials on a variety of investigative matters, including IP-related investigations. Recognizing the significance of the IP threat in China, the FBI conducted a threat assessment and sent an agent and an analyst to China to meet with local government and industry representatives. The information obtained through these activities was a factor in the decision to deploy a dedicated IP agent to Beijing to work closely with Chinese law enforcement officials on IP matters of joint interest.

**23. From the reports submitted by the IPEC, DOJ and FBI, it appears a majority of the cases involve Chinese products seized and/or Chinese defendants. Do you feel there has been a corresponding decrease in cases involving China since the meetings between American and Chinese officials took place last fall? Why?****Response:**

Statistics that would demonstrate a recent decline or increase in cases involving China are not readily available at this time. However, informal observation indicates that the number of investigations may be fairly constant. While the meetings may have resulted in greater Chinese enforcement efforts and fewer violations, we may be pursuing a greater portion of these violations as a direct consequence of the greater investigative resources devoted to IPR infringements. In addition, or in the alternative, continued growth in the Chinese economy, both legitimate and illegitimate, may be negating any enforcement progress made by China since last fall's meetings.

**24. What else needs to be done to decrease the infringement threat from China?**


---

*These responses are current as of 9/13/11*

**Response:**

Continuing to engage our Chinese law enforcement counterparts and strengthening those relationships are critical to decreasing the IPR infringement threat posed by China. This engagement, which should include information sharing and joint criminal enforcement operations, will be enhanced when the FBI's dedicated IP agent arrives in Beijing later this year. Joint training opportunities that include both U.S. and Chinese law enforcement officers should also be aggressively pursued, and innovative ideas, such as a Chinese-based IPR enforcement academy, should be thoroughly evaluated.

---

*These responses are current as of 9/13/17*



RESPONSES OF ERIK BARNETT TO QUESTIONS SUBMITTED BY SENATORS GRASSLEY,  
COBURN, AND FRANKEN

<b>Question#:</b>	1
<b>Topic:</b>	IP
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Response:** Civil fines and penalties are not fees. A fine or penalty is established when a violation of import/export law is discovered. When intellectual property rights (IPR) penalties are collected, the monies are deposited in the Treasury General Fund as revenue. The collected penalty amounts are not used to offset CBP's seizure costs.

CBP does recover some seizure costs from the Department of the Treasury Forfeiture Fund (TFF), which was established under section 9703.1, Title 31, United States Code (31 U.S.C. § 9703.1). The TFF provides for the payment of all proper expenses of seizure (including investigative costs incurred by a TFF law enforcement organization leading to seizure) or to the proceedings of forfeiture and sale, including the expenses of detention, inventory, security, maintenance, advertising, or disposal of property ...” In accordance with the United States Code, fines and penalties are not deposited into the TFF.

<b>Question#:</b>	2
<b>Topic:</b>	GAO report
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** The 2008 GAO Report also noted CBP had not been analyzing the variations in its IP enforcement activity by port, or how successful each port has been in enforcement. Does CBP now examine IP enforcement by port? Why or why not?

**Response:** CBP analyzes enforcement data, including IPR enforcement data, by a variety of factors. Publicly, CBP publishes annual IPR seizure data that includes breakouts by various factors, including trends such as the type of transaction as commercial or consumer, and the environment in which it occurs, such as mail, express or commercial cargo. Internally, CBP analyzes IPR enforcement data on a number of additional factors, including by port, all in order to monitor major trends and shifts in IPR violations. CBP has monitored this data nationally and by port since approximately 2001, and has mechanisms for analyzing this data from headquarters (HQ) to the field, as well as for the field to monitor itself.

**Question:** If you do not, how can CBP be effective in allocating its limited resources and improving the use of those resources at ports that may not be performing as they should?

**Response:** n/a

<b>Question#:</b>	3
<b>Topic:</b>	IPEC's
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** The IPEC's 2010 Annual Report notes the number of consumer safety and critical technology seizures at CBP increased 97%. Is this because public health and safety seizures were not a priority in the past or because of more importation of these types of products?

**Response:** The increase in consumer safety and critical technology seizures in fiscal year 2010 can be attributed to several factors. CBP and U.S. Immigration and Customs Enforcement have placed an increased emphasis on enforcing consumer safety and critical technology intellectual property violations. Greater enforcement against counterfeit products sold over the internet and shipped through mail and express courier facilities resulted in high-volume, low-value seizures. In addition, rights holders provided more training to CBP officers in these facilities to help them identify counterfeits.

**Question:** For how long have these types of seizures been a priority at CBP?

**Response:** Enforcement against products posing safety and security threats has long been a priority at CBP. We have been seizing these types of products since the 1990's. We began reporting on our increased focus in this area in 2007.

<b>Question#:</b>	4
<b>Topic:</b>	pilot program
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** You note in your testimony that CBP has a Center for Excellence and Expertise, which is a pilot program focused on the pharmaceutical industry.

How does this program coordinate with the IPEC's working group on counterfeit pharmaceuticals?

**Response:** CBP was an integral member of the Intellectual Property Enforcement Coordinator's (IPEC) working group on counterfeit pharmaceuticals, helping to develop the Administration's plans for protecting American consumers against counterfeit medicines. The working group's report, which was sent to the Vice President and Congress in March 2011, includes CBP's Pharmaceutical Center for Excellence and Expertise (CEE) as one action the Administration is taking. The CEE's mission includes expanding the Agency's knowledge base about the pharmaceutical industry, creating a centralized source of expertise for pharmaceuticals, driving uniform implementation of policies and procedures, and working with the U.S. Food and Drug Administration (FDA) to improve targeting for counterfeit, substandard, and unapproved drugs.

<b>Question#:</b>	5
<b>Topic:</b>	Law
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** Are there any additional tools that you'd like to see enacted into law that would assist you in your efforts to protect intellectual property rights, both here and abroad?

**Response:** In implementing the Administration's Joint Strategic Plan for IPR Enforcement, CBP worked with the IPEC on a comprehensive review of laws. IPEC issued a White Paper on Legislative Recommendations in March 2011 suggesting several legal authorities to enhance CBP's ability to protect IPR. A key recommendation would assist CBP with the challenge of determining whether a product is counterfeit or genuine. As the quality of counterfeit goods improves, it is increasingly difficult for CBP to make infringement determinations. Rights holders are the experts in their products and CBP values the information that rights holders can provide to assist CBP with infringement determinations. CBP is seeking passage of its legislative initiative which would provide the Agency with authority to share information contained on samples of suspected counterfeit and pirated goods with rights holders prior to seizure to assist infringement determinations.

<b>Question#:</b>	6
<b>Topic:</b>	resources
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** The federal government has a finite number of resources to conduct its law enforcement investigations and prosecutions. Yet piracy and counterfeiting are surging all over the world, as well as online. Do you think that rights holder actions can alleviate some of the burdens on federal law enforcement and effectively combat IP theft?

**Response:** CBP has excellent working partnerships with many rights holders who take the steps necessary to help CBP enforce their rights, including recording their rights with CBP, working with CBP to conduct port training to help our officers recognize counterfeit products, providing reference materials to CBP, which are posted on CBP's intranet and accessible to CBP employees, and submitting allegations of infringement through e-Allegations, CBP's online repository for allegations relating to violations of the customs laws.

While many rights holders do partner with CBP, many also do not, for different reasons. These include lack of resources on the part of rights holders, and in some cases, lack of knowledge on the part of rights holders that taking these fairly simple and straightforward steps can greatly enhance CBP's ability to target, detain, and seize counterfeit goods. CBP actively encourages rights holders to partner with CBP by taking these steps. Rights holders should also provide a knowledgeable contact who can respond timely to inquiries from CBP when suspect goods are detained, and should keep contact information current in CBP's recordation system.

CBP is working to develop IPR supply and distribution chain management programs as described in CBP's Five-Year IPR Strategy submitted to Congress in 2010. This program would expand CBP's partnership with the rights holders and importers in order to enhance CBP's risk analysis and targeting of shipments at high risk for IPR infringing goods while expediting the release into commerce of low risk shipments. CBP is actively seeking to encourage rights holders and importers to participate in the dialogue as we develop these programs because the success of these programs are dependant on significant input and buy-in from the private sector. Successful programs will be advantageous to rights holders and importers as well as to CBP. CBP's IPR enforcement would benefit from better targeting efficiency, which would lead to increased seizures. Importers would benefit from reduced costs associated with unnecessary inspections and the greater predictability in their supply chains that would result from increased targeting efficiency. Rights holders would benefit from the increased protection of their rights enabled by CBP's increased targeting efficiency.

<b>Question#:</b>	6
<b>Topic:</b>	Resources
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

High quality counterfeit and pirated goods make IPR infringement determinations challenging, and many rights holders use overt and covert technologies for authentication purposes. However, when CBP is authenticating goods and making infringement determinations, it is impractical for the agency to know and employ the numerous technologies used by rights holders. Presently, approximately 25,000 trademarks and copyrights are recorded with CBP. Greater uniformity and standardization of authentication tools and technologies used to identify infringement of these rights would assist CBP in making infringement determinations.

Rights holders could help CBP and law enforcement to educate consumers and businesses about IPR infringement as this is as important step in the fight against counterfeiting and piracy both in the United States and overseas. If there are fewer consumers of counterfeit and pirated goods, there will be less production. There are also actions outside of the United States that rights holders can take such as working with foreign governments to deliver training.

<b>Question#:</b>	7
<b>Topic:</b>	Civil penalties
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** In your opinion, how effective are civil penalties as an enforcement tool at the border, as opposed to criminal prosecutions by the Department of Justice?

**Response:** The Department of Homeland Security (DHS), through CBP and U.S. Immigration and Customs Enforcement (ICE), has worked with the Department of Justice (DOJ) in collecting civil penalties and in administering criminal IPR prosecutions. Civil penalties and criminal prosecutions complement each other and each process serves as an effective enforcement tool. There are, however, benefits and drawbacks with respect to using either process.

Successful criminal prosecutions result in the incarceration of willful IPR violators and the seizure of any assets that the violator accrued through his or her criminal actions. Criminal prosecutions are public. DOJ provides announcements advising the public of criminal indictments for IPR violators and of its successful criminal convictions. These announcements, which tell the public that the Government is serious about prosecuting trademark and copyright violators and that the courts are willing to impose stiff penalties against those parties, serve as a deterrent to the importation of IPR infringing goods. Conversely, criminal prosecutions are expensive and can divert valuable resources away from the investigation of narcotics violations, terrorism, and violent crimes. Successful civil penalties encourage negligent and unintentional importers of IPR infringing goods to adopt business practices that are consistent with the law, result in the collection of assessed or mitigated penalty amounts, and generate revenue for the Government. Civil penalties are less burdensome for the Government to process than criminal prosecutions because there are no *mens rea* requirements associated with the penalty. Unfortunately, the absence of *mens rea* requirements also makes it difficult for CBP to publish the names of the penalized parties. This limits the multiplying effect that is garnered from criminal prosecutions because the public is not privy to information regarding the effects of the penalty. Penalties that must be presented to DOJ for collections require significantly more time and resources to process, but the Government, if it prevails on the claim, would be able to collect the fully assessed penalty amount.

#### BACKGROUND:

Many of the criminal IPR cases that DOJ prosecutes stem from CBP's civil administrative seizure cases. In the criminal prosecutions, CBP employees, including, but not limited to auditors, attorneys, CBP Officers, Fines, Penalties and Forfeitures Officers, Import Specialists, and Seized Property Specialists may assist to process the



<b>Question#:</b>	7
<b>Topic:</b>	civil penalties
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

underlying civil seizure—by reviewing the underlying IPR infringement determination, valuing the merchandise, ensuring the viability of the underlying seizure, and maintaining the seized property—while ICE Special Agents work closely with DOJ in continuing the underlying criminal investigation.

CBP is also a leading source of referrals to ICE for possible criminal investigations of IPR infringements. As a participating agency in the National Intellectual Property Rights Coordination Center (IPR Center), CBP leverages our targeting and interdiction successes to contribute to special operations. For example, CBP, in conjunction with the Federal Bureau of Investigation (FBI) and ICE, initiated Operation Network Raider in May 2010, which targets the illegal distribution of counterfeit network hardware manufactured in China. To date, referrals from this operation to ICE for criminal investigation have resulted in 30 felony convictions and 700 seizures of counterfeit Cisco network hardware. CBP is also participating in the recently announced IPR Center Operation Chain Reaction, a multi-agency effort to protect the military's supply chain from being infiltrated by counterfeit goods. In one recent criminal prosecution charging 18 U.S.C. § 2320 (trafficking in counterfeit goods) *U.S. v. Chong Lam and Joyce Chen*, CBP is now pursuing three civil penalties that were assessed under 19 U.S.C. § 1526(f), against the convicted criminal counterfeiters.

Although it has been difficult to collect civil penalties based on the manufacturer's suggested retail price, recent victories in the district courts may lead to greater collections as violators achieve a greater awareness that the government is serious about pursuing uncollected penalties. The Government has successfully litigated three civil penalties that were assessed under 19 U.S.C. § 1526(f). The cases are *United States v. Nguyen*, in which the violator was required to pay the fully assessed penalty amount and to pay much of the Government's attorney fees; *Able Time v. United States*, which affirmed the Government's ability to assess penalties under 19 U.S.C. § 1526(f) and required the violator to pay the assessed penalty amount; and *Sakar v. United States*, which was remanded to the U.S. Court of International Trade for dismissal, because the U.S. Court of Appeals for the Federal Circuit determined that the CIT did not have jurisdiction over penalties assessed under 19 U.S.C. § 1526(f). The awarding of the administrative penalty, which is again under review with CBP, affirmed the Government's position that penalties assessed under section 1526(f) were within the district courts jurisdiction. CBP is working to enhance the quality of the civil IPR penalty cases that it refers to DOJ for judicial collections.

<b>Question#:</b>	8
<b>Topic:</b>	increase
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** Your testimony describes efforts to increase the number and severity of civil penalties. Is this proving to be a successful deterrent?

**Response:** CBP has taken preliminary steps to amend Treasury Decision 99-76 (T.D.), which will permit the issuance of a civil penalty pursuant to 19 U.S.C. 1526(f) to be assessed against any party who directs, assists financially or otherwise, aids or abets in the importation of merchandise seized under 19 U.S.C. 1526(e) at the domestic value, rather than the MSRP of the genuine article. It is CBP's position that assessing penalties at the domestic value would increase the penalty collection rates. This proposed policy will permit CBP Fines, Penalties, and Forfeitures Officers to assess civil fines at the domestic value of the merchandise seized for the first violation, and at not less than two times the domestic value and not more than the MSRP for the second and subsequent violations where CBP has previously assessed a civil penalty and the civil penalties will be issued concurrently with the seizure.

To deter IPR violators, CBP will continue to collaborate with ICE to identify assets that could be pursued for collection on IPR penalties. Additionally, in September 2011, CBP will be conducting an IPR Enforcement Conference for key field personnel which will add to our goal of increasing and improving the effectiveness of various trade enforcement processes and actions, including deterring IPR infringement and enforcing IPRs ; protecting the public from hazardous imports through effective Import Safety enforcement; increasing the penalties imposed on entities that attempt to defraud the U.S. government out of duties due through the use of our penalty provision; and improving the lines of communication among the front-line CBP field personnel and various components within CBP and ICE Headquarters.

<b>Question#:</b>	9
<b>Topic:</b>	negotiations
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** Are you obtaining adequate cooperation from the Chinese government with regard to your ongoing negotiations? What are the prospects for actually improving customs enforcement through these negotiations?

**Response:** As described below, CBP conducts on-going negotiations with the Chinese government, reaches out to in-country organizations, and coordinates training opportunities with the Chinese government. Cooperation from the Chinese government has been sufficient to allow us to complete negotiations on two MOUs.

#### Negotiations

CBP signed a Memorandum of Cooperation (MOC) with the General Administration of China Customs (GACC) in May 2007 that created a framework for cooperation to enhance border enforcement of IPR between China and the United States. The MOC provides for sharing import information, sharing best practices, exchanging personnel and experiences, and engaging cooperatively with industry. On May 9, 2011, CBP and GACC signed and exchanged letters amending the MOC on Strengthening Cooperation in Border Enforcement of Intellectual Property Rights. The exchange was completed on the margins of the Strategic & Economic Dialogue (S&ED) to improve the information sharing provisions of the MOC.

Also on the margins of the May S&ED, CBP signed a Memorandum of Understanding (MOU) Regarding Cooperation in Law Enforcement Matters with the Ministry of Public Security (MPS) of the People's Republic of China. Among other things, the MOU provides for cooperation with MPS on IPR enforcement.

The prospect for improving customs enforcement beyond signing MOUs is yet to be determined and may be highly dependent upon the successful execution of follow-on action plans that focus on specific intellectual property rights such as copyright or trademark and identify specific goals and results.

#### Outreach and Developments

CBP Beijing, as part of the U.S. Mission's Intellectual Property (IP) Working Group, has participated in outreach to the American Chamber of Commerce of China (AmCham – China) and the Quality Brands Protection Committee (QBPC); and on June 24, 2011, attended the 11<sup>th</sup> Anniversary of Quality Brands Protection Committee of China Association of enterprises with Foreign Investment (CAEFI) which included the Recognition Ceremonies for 2010-2011 China IPR Best Practices and the Outstanding

<b>Question#:</b>	9
<b>Topic:</b>	negotiations
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

Agencies for Nation-wide Enforcement Operation. Such in-country organizations have well intentioned plans of protecting U.S. brands mainly inside the Chinese internal market. Members include many Fortune 500 companies. An effective IP protection agenda must bring together the brand owners, the business community and government authorities to include the law enforcement community and prosecutors.

#### Training Coordination

CBP Beijing has worked with GACC to nominate four attendees to the International Law Enforcement Academy's (ILEA) Seaport Interdiction / Cargo Targeting course held from June 6 – 17, 2011. These CBP sessions not only provide knowledge and relationship building, but also provide credibility for the Agency's efforts.

CBP Beijing worked with the Embassy Beijing Economics Section, U.S. Patent and Trademark Office (USPTO), and ICE Beijing to invite officials from MPS, GACC, and the Supreme People's Court (SPC) to attend State funded US – China – Japan intellectual property enforcement seminar scheduled for the first week of September 2011 at Qingdao, China. If all goes well and the seminar is ultimately conducted, the seminar will be the first U.S.-led forum that has had the ability to bring the legal and enforcement sides together. In late July, the proposed event was postponed in order to comply with the Leahy Amendments linked to the Bureau for International Narcotics and Law Enforcement Affairs (INL). The group is looking for an alternative training site outside China before offering the seminar to a wider spectrum of attendees from additional regional countries.

<b>Question#:</b>	10
<b>Topic:</b>	training programs
<b>Hearing:</b>	Oversight of Intellectual Property Law enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** The 2010 IPEC report mentions CBP's involvement in training programs in Africa, Europe, and other nations. How extensively is CBP involved in international training programs? What is the general substance of those trainings?

**Response:** Foreign IPR training is typically funded by the Department of State and conducted through other agencies, notably the U.S. Patent and Trademark Office and the Commercial Law Development Program at the Department of Commerce. CBP has been actively engaged in these IPR training programs by providing subject matter experts in the areas of targeting, risk management, border interdiction techniques, and legal aspects and issues in IPR enforcement.

In the last twelve months, CBP provided trainers for 11 programs conducted in El Salvador, Hong Kong, India, Mexico, Morocco, Russia, Thailand (twice), Trinidad and Tobago, Uganda, and Ukraine.

<b>Question#:</b>	1
<b>Topic:</b>	Protect IP
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** As you know, the Judiciary Committee passed the PROTECT IP Act last month in an effort to provide the federal government more tools to address the growing problem of rogue websites that are dedicated to infringing activity. Since you have not testified in the Senate on that legislation, could you please explain your position on the bill, whether it duplicates the existing Operation in Our Sites initiatives you have been performing, why you need additional authority in the bill, and whether you think the legislation will be effective in shutting down these websites.

**Response:** U.S. Immigration and Customs Enforcement (ICE) defers to Office of Management and Budget (OMB) and the Intellectual Property Enforcement Coordinator (IPEC) for comment on the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property (PROTECT IP) Act.

**Question:** Under the current Operation in Our Sites, on average, how many (or what percentage of) websites removed during those operations re-appear in another form after being shut down?

**Response:** ICE does not maintain statistics of the average number of websites that reappear after domain names are seized pursuant to court orders obtained through Operation In Our Sites. However, of the first nine domain names seized—that were engaged in online piracy of movies, music, and software—we are aware of only two that reappeared in another form, and one of those was re-seized later in 2010. Operation In Our Sites v. 2.0 primarily targeted counterfeit goods sold on the internet and was timed with Cyber Monday, billed as the largest online shopping day of the year. That operation resulted in the seizure of 77 domain names of websites, all based in China. We are aware that a portion of those sites reappeared in some other form. The operators of these sites, of course, are part of an organization that has an inventory of counterfeit goods and the internet has become a favored vehicle for distribution. Overall, ICE has become aware of other websites reappearing in some other format after the three subsequent phases of Operation In Our Sites. However, after the first round of Operation In Our Sites, ICE also learned that 81 websites that had previously been engaged in online piracy of copyrighted movies and television shows voluntarily stopped offering such illegal content. Further, even if a website does re-appear with a different domain name, it must build up traffic to the site to become profitable from advertising and other revenue. The targets of Operation In Our Sites are all commercial sites, that is, they exist to earn profit from criminal activity. Therefore, Operation In Our Sites disrupted the criminal activity

<b>Question#:</b>	1
<b>Topic:</b>	Protect IP
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

by denying the profit. Admittedly, what Operation In Our Sites cannot do is target sites for which the domain names are not administered in the United States..

**Question:** When conducting Operation in Our Sites, on average, how many (or what percentage of) websites are targeted because of their effect on public health and safety?

**Response:** Operation in Our Sites was created by ICE, and is programmatically managed at ICE's National Intellectual Property Rights (IPR) Coordination Center, to target four major types of counterfeiting and copyright violations carried out on the internet: piracy of movies and music; pharmaceuticals; other IPR violations impacting health and safety; and piracy of electronic devices and games (software). Of the 125 domain names seized, 18 can be directly associated with violations that involved public health and safety. This represents 14 percent of the domain name seizures under Operation In Our Sites to date. But this is an ongoing operation with three phases already completed in 2011 and more planned.

<b>Question#:</b>	2
<b>Topic:</b>	GAO
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** In 2008, GAO reported that ICE planned to move the IPR Center and its relocation would be an opportunity to return the center to its original concept and purpose. Do you believe the IPR Center has returned to an appropriate focus as an effective coordination center?

**Response:** Yes. The National Intellectual Property Rights Coordination Center (IPR Center) brings together 17 key federal investigative member agencies, and the governments of Canada and Mexico in a task force setting. The task force structure enables the IPR Center to efficiently and effectively leverage the resources, skills, and authorities of each participating agency and government, and provides a comprehensive response to intellectual property (IP) theft, resulting in “one-stop shopping” for IPR law enforcement and industry in the United States and around the world. Cooperation among IPR Center partners has continued to grow over the past year, with member agencies participating in several joint operations and investigations. This cooperation includes the recently announced Operation Chain Reaction, in which nine IPR Center partner agencies and prosecutors from the Department of Justice (DOJ) are working together to target counterfeit items entering the supply chains of the Department of Defense and other U.S. Government agencies.

In addition, the IPR Center recently added several agencies to more comprehensively address the mission of the IPR Center to combat predatory and unfair trade practices that threaten our economic stability and national security, undermine the competitiveness of U.S. industry in world markets, and place the public’s health and safety at risk.

Thus far in 2011, the IPR Center has welcomed the following new partners: the U.S. Consumer Product Safety Commission; the Defense Logistics Agency, Office of Inspector General; the U.S. Department of State, Office of International Intellectual Property Enforcement; the U.S. Air Force, Office of Special Investigations; the National Aeronautics and Space Administration, Office of the Inspector General; and our second international partner, the Royal Canadian Mounted Police. While DOJ is not an official partner at the IPR Center, federal prosecutors work closely with all agency partners at the IPR Center. As noted above, this close relationship has contributed to the IPR Center’s goal of establishing a “one-stop shop” for IP theft victims and industry, reducing duplication, and allowing us to leverage and benefit from our unique missions and different areas of expertise.



<b>Question#:</b>	2
<b>Topic:</b>	GAO
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** How does the IPR Center coordinate with other agencies and de-conflict cases?

**Response:** The IPR Center was created to share information and to promote a coordinated U.S. Government response to IP theft. The IPR Center provides one-stop shopping for IPR law enforcement and industry in the United States and around the world. The IPR Center utilizes a multi-layered approach to investigate, interdict, and prosecute criminals engaged in IP theft.

Investigative case referrals and leads to IPR Center partner agencies are researched and reviewed by all partners through a process called vetting and de-confliction. When leads are received directly by the IPR Center, intelligence reports are first generated from those leads as part of the “vetting” process. Leads are distributed to all partner agencies and the DOJ Computer Crime and Intellectual Property Section to determine whether an agency is already investigating the alleged IP violation. Information from agencies’ active cases is also shared with the partner agencies in a process called “de-confliction” to determine whether multiple agencies have an interest in the same target. All IPR Center partners meet weekly to review the results of this vetting and de-confliction process and to establish which partner agency or agencies will be responsible for determining future action on leads. The lead partner agency then coordinates with the IPR Center to ensure any further enforcement action is tracked, monitored, de-conflicted, and reported to IPR Center partners. IPR Center partner agencies also share information acquired from their investigations including information about emerging criminal trends, and information about new technologies that infringers are using.

**Question:** Has it been successful in preventing unneeded overlap in various agencies dealing with IP enforcement? How?

**Response:** The IPR Center is a repository and gateway for most IP investigative case referrals, particularly from American manufacturers and rights holders. If the de-confliction process reveals that an agency is investigating a case or has dedicated significant agency resources, consideration will be given to how to handle an investigation in order to avoid duplication of resources and waste. In fiscal year (FY) 2010, the IPR Center vetted more than 240 potentially actionable leads received and de-conflicted 544 leads from IPR Center partner agency investigations. From the beginning of FY 2011 through May 31, 2011, the IPR Center has vetted 150 leads and de-conflicted 849 leads. In addition, IPR Center partner agencies share information acquired from their investigations, including information about emerging criminal trends, and information about new technologies used in infringement. All of these efforts have made the U.S. Government more efficient at enforcing IP theft.

<b>Question#:</b>	3
<b>Topic:</b>	IPEC
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** According to reports from the Office of the Intellectual Property Enforcement Coordinator (IPEC), ICE entered into agreements with China and Korea to cooperate between enforcement agencies to combat IP crime and money laundering. What steps have those countries taken to fulfill these agreements? Do you feel these agreements have been effective to-date?

**Response:** ICE has not seen significant steps taken to increase enforcement actions or cooperation between the U.S. and China on money laundering or intellectual property violations since Director Morton signed a Memorandum of Understanding (MOU) with the Ministry of Public Security. ICE would like to see more complete responses from Chinese authorities when ICE requests assistance on investigations. ICE also wished to have leads and requests for joint investigations in China followed up on and results shared with ICE. One bright note has been the increased cooperation between Guangdong and Fujian China Inspection and Quarantine Bureau (CIQ) and ICE. CIQ has expressed increased interest in investigating products with a safety nexus, including electronic products that contain counterfeit certification labels, such as counterfeits of labels that the Underwriters Laboratories (UL) issues. After several initial meetings with CIQ, CIQ is now actively reaching out to ICE for leads on manufacturers and shippers of goods containing counterfeit UL labels, and possibly joint criminal investigations to be conducted in Guangdong province. Outside of Guangzhou CIQ, cooperation seems to occur typically when ICE is requested to provide information and/or assistance to Chinese authorities as part of an ongoing domestic (Chinese) investigation.

In September 2010, ICE and the Supreme Prosecution Service (SPS) of the Republic of Korea signed a MOU, which includes a provision on cooperation in the areas of anti-money laundering and intellectual property rights (IPR). Prior to this agreement, the SPS and ICE already conducted joint investigations; the MOU served to formalize the cooperation. The SPS and ICE continue to conduct joint IPR investigations and there has been an increase in leads/referrals from the SPS for potential money laundering investigations. ICE considers this agreement effective thus far.

<b>Question#:</b>	4
<b>Topic:</b>	enforcement
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** Could you each explain briefly your responsibilities in IP enforcement and how you coordinate with one another?

**Response:** U.S. Immigration and Customs Enforcement (ICE) is a leading agency in the investigation of criminal intellectual property (IP) violations involving the illegal production, smuggling, and distribution of counterfeit and pirated products, as well as associated money laundering violations. With regard to counterfeit goods entering the United States through ports of entry, ICE targets and investigates individuals and criminal enterprises and also seizes, for forfeiture, goods associated with these investigations, including goods that infringe trademarks, trade names, and copyrights. With regard to copyright violations, a large portion of these crimes now occur over the internet. ICE investigates copyright violations and, together with the Department of Justice, has seized domain names of websites engaging in copyright violations as well as trademark counterfeiting. ICE has also seized assets of criminal organizations and instrumentalities of the criminal activity. In FY 2010, ICE's Homeland Security Investigations (HSI) directorate initiated 1033 IP theft enforcement cases, a 42 percent increase over FY 2009. HSI agents also worked 281,218 investigate hours on IP theft enforcement cases in FY 2010, a 27 percent increase over FY 2009.

However, ICE HSI recognizes that no single U.S. law enforcement agency can succeed alone against IP theft. Rather, it is essential that all relevant federal agencies work together and with rights holders to confront this challenge. Therefore, ICE HSI initiated the National Intellectual Property Rights Coordination Center (IPR Center) to efficiently and effectively leverage the resources, skills, and authorities of each participating agency. The IPR Center promotes coordination and communication among 17 key federal investigative agencies and the governments of Canada and Mexico with roles in enforcing IP laws, through the mechanism of a task force concept. The task force structure enables the IPR Center to provide a comprehensive response to IP theft, resulting in one-stop shopping for IPR law enforcement and for rights holders in the United States and around the world.

Investigative case referrals and leads to IPR Center partner agencies are researched and reviewed by all partners through a process called de-confliction. When leads are received directly by the IPR Center, intelligence reports are first generated from those leads as part of the vetting process. Leads and case referrals from partner agencies are distributed to all partner agencies and the Department of Justice Computer Crime and Intellectual Property Section for vetting and de-confliction to determine whether an agency is already

<b>Question#:</b>	4
<b>Topic:</b>	enforcement
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

investigating the alleged IPR violation. All IPR Center partners meet weekly to review the results of this de-confliction process and to establish which partner agency or agencies will be responsible for determining future action on that lead. The lead partner agency then coordinates with the IPR Center to ensure any further enforcement action is tracked, monitored, de-conflicted and reported to IPR Center partners.

<b>Question#:</b>	5
<b>Topic:</b>	IPR Center
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** How effective has the IPR Center been at coordinating agency efforts and de-conflicting cases to ensure no duplication occurs?

**Response:** ICE believes the IPR Center has been very effective at coordinating agency efforts and at de-conflicting cases to ensure that no duplication occurs. The IPR Center was created to share information and promote a coordinated U.S. Government response to intellectual property (IP) theft. The IPR Center provides one-stop shopping for IPR law enforcement and industry in the United States and around the world utilizing a multi-layered approach to investigate, interdict, and prosecute criminals engaged in IP theft.

Investigative case referrals and leads to IPR Center partner agencies are researched and reviewed by all partners through a process called de-confliction. When leads are received directly by the IPR Center, intelligence reports are first generated from those leads as part of the vetting process. Leads and case referrals from partner agencies are distributed to all partner agencies and the Department of Justice Computer Crime and Intellectual Property Section for vetting and de-confliction to determine whether an agency is already investigating the alleged IP violation. All IPR Center partners meet weekly to review the results of this de-confliction process and to establish which partner agency or agencies will be responsible for determining future action on that lead. The lead partner agency then coordinates with the IPR Center to ensure that any further enforcement action is tracked, monitored, de-conflicted and reported to IPR Center partners. IPR Center partner agencies also share information acquired from their investigations such as emerging criminal trends and information about new technologies that infringers utilize.

The success of the IPR Center is not due to any single agency, but rather to the combined and sustained commitment of each individual partner agency to conduct a collegial and effective coordination process.

<b>Question#:</b>	6
<b>Topic:</b>	agencies
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** How does each of your agencies coordinate with private industry to improve your enforcement efforts?

How has the private industry stepped up their efforts to enforce their rights and coordinate with the federal government?

**Response:** For ICE's Homeland Security Investigations (HSI), coordination with industry is achieved through Operation Joint Venture, an outreach initiative coordinated through the National Intellectual Property Rights Coordination Center (IPR Center). Operation Joint Venture aims to increase information sharing with public and private sectors to combat the illegal importation and distribution of counterfeit, substandard, and tainted goods. Operation Joint Venture reaches rights holders, manufacturers, importers, customs brokers, freight forwarders, bonded facilities, carriers, and others to discuss the IPR Center's priorities of protecting public health and safety, the economy and the war fighter. Since July 2008, the IPR Center and ICE HSI agents have led or participated in approximately 638 outreach events, including formal presentations and meetings, speaking with approximately 34,078 people.

Through the IPR Center's aggressive outreach efforts, ICE ensures that rights holders understand: (1) to whom and how to report a potential intellectual property crime; (2) the types of cases generally accepted by the U.S. Government for criminal prosecution in intellectual property cases; and (3) information that victims and rights holders should provide to assist law enforcement in developing an intellectual property case. The IPR Center ensures communication with rights holders during criminal investigations, subject to the limitations imposed by the government's legal, ethical, and law enforcement obligations. This can enable rights holders to seek civil remedies, including in cases where a lead is declined for investigation.

**Question:** How has the private industry stepped up their efforts to enforce their rights and coordinate with the federal government?

**Response:** Private industry from all sectors routinely visit the IPR Center to discuss the latest industry trends related to IP theft and provide information and leads that can be utilized by ICE and other partner agencies to initiate criminal investigations and national initiatives. Leads that do not meet the threshold for criminal investigations or initiatives are referred back to private industry, who may pursue civil action against the violators. The increased activity over the past two years of U.S. law enforcement and other federal

<b>Question#:</b>	6
<b>Topic:</b>	agencies
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

agencies, including efforts coordinated by the Intellectual Property Enforcement Coordinator (IPEC), seems to have spurred private industry to greater efforts to enforce their rights and to coordinate with the federal government. The IPEC has also achieved great success through encouraging voluntary cooperation among stakeholders to reduce IP theft.

<b>Question#:</b>	7
<b>Topic:</b>	Pro-IP Act
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** How much does each of your agencies spend annually on IP enforcement? Has that increased since the passage of the PRO-IP Act in 2008?

**Response:** ICE's Homeland Security Investigations (HSI) estimates it will spend approximately \$50 million for IP theft enforcement in FY 2011, based upon the amounts spent as of the second quarter of the fiscal year. The spending by HSI for IP theft enforcement for the fiscal years since the passage of the PRO-IP Act is set out below. Expenditures on IP theft enforcement have generally increased since the passage of the PRO-IP Act of 2008 although HSI does not budget specifically for particular investigative missions and instead allows crime trends and agency priorities determine resource allocation. In the FY 2010 budget, the President did request, and Congress approved, \$5 million for the IPR Center. Otherwise, all funding for IP theft enforcement by HSI is part of ICE's base investigatory budget.

FY 2008 – \$27.699M

FY 2009 – \$32.237M

FY 2010 – \$42.643M

FY 2011 – \$27.785M (as of the end of the 2nd quarter of FY 2011).



<b>Question#:</b>	8
<b>Topic:</b>	amount
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** Has the amount and/or quality of agency coordination improved since the formation of the Office of the IP Enforcement Coordinator in 2009? Why or why not?

**Response:** Yes, the amount and/or quality of agency coordination has greatly improved since the formation of the Office of the IP Enforcement Coordinator (IPEC) in 2009. The IPEC has assisted in the coordination between agencies on a number of matters including legislative recommendations, international efforts to curb IP theft, and other important areas. The IPEC has also raised the profile of intellectual property (IP) crime within the federal government and the private sector.

Since the issuance of the IPEC's Joint Strategic Plan in June 2010, ICE's Homeland Security Investigations and the National Intellectual Property Rights Coordination Center (IPR Center) have worked closely with the IPEC to aggressively implement the strategy, including by participating in a series of IPEC-led interagency working groups and through development of several reports to Congress and President Obama and Vice President Biden. These actions have led to increased coordination in IP enforcement policy, which complements the efforts of the IPR Center to increase coordination on enforcing criminal laws against IP theft.

<b>Question#:</b>	9
<b>Topic:</b>	products
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** Are there certain products or offenses that dominate your enforcement efforts?

**Response:** The intellectual property (IP) theft enforcement of ICE's Homeland Security Investigations (HSI) most often pertain to the importation and trafficking of counterfeit goods, also known as "hard goods." These enforcement efforts target a wide range of counterfeit products, including pharmaceuticals, clothing, consumer electronics, critical technical components, electrical articles, electronic media, eyewear, footwear, luxury goods, and cigarettes.

Historically, counterfeit goods were smuggled into the U.S. in bulk shipments utilizing sea containers, and were typically sold at storefronts or by street vendors. While ICE HSI still sees IP theft occurring through these means, criminal organizations involved in IP theft are now increasingly using the Internet to distribute counterfeit trademarked goods and copyrighted content. Foreign-based IP smuggling organizations are also shifting their shipping methods to express consignment couriers and mail services to send smaller amounts of their products directly to purchasers.

<b>Question#:</b>	10
<b>Topic:</b>	property
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** Are there certain countries that pose more serious threats to American intellectual property than others?

**Response:** While the criminal activity of IP theft is seen in many countries, the level of such activity is greater in some countries. For instance, in FY 2010, U.S. Customs and Border Protection (CBP) and ICE's Homeland Security Investigations (HSI) seized goods with a domestic value of \$124,681,247 from China; \$26,173,057 from Hong Kong; \$7,713,398 from Jordan; \$1,571,142 from India, and \$1,286,373 from Malaysia. Seizures of goods originating from all other countries had a combined domestic value of \$26,700,129, approximately one-fifth of the amount attributable to seized goods from China. The domestic value represents the cost of the merchandise when last purchased, plus all duties, fees, broker's charges, profit unloading charges, and U.S. freight charges to bring the property to the importers premises; the manufacturer's suggested retail price (MSRP) is the value the counterfeit goods would have sold at retail if they had been genuine. The MSRP for FY 2010 IPR seizures by CBP and HSI was \$1.4 billion.

<b>Question#:</b>	11
<b>Topic:</b>	China
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** What kind of discussions have you been having with China?

From the reports submitted by the IPEC, DOJ and FBI, it appears a majority of the cases involve Chinese products seized and/or Chinese defendants. Do you feel there has been a corresponding decrease in cases involving China since the meetings between American and Chinese officials took place last fall? Why?

What else needs to be done to decrease the infringement threat from China?

**Response:** The criminal investigations of ICE's Homeland Security Investigations (HSI) often uncover criminal operatives and organizations overseas. This is especially true in intellectual property theft enforcement because there is almost no "purely" domestic intellectual property theft.

Therefore, ICE's HSI must have "boots on the ground" to work with foreign law enforcement. HSI has the largest presence of a U.S. law enforcement agency in China, with offices in Beijing and Guangzhou, as well as Hong Kong. Our Assistant Attaché in Guangzhou has been designated ICE's first "IP Attaché" and ICE's point of contact for all IP matters involving China.

China continues to be the primary source country for intellectual property theft involving products exported to the United States, as it has been for the last 10 years. When comparing data from May and June of 2010 and 2011, respectively, seizures of counterfeit goods from China entering the United States have remained the same. In 2011, seizures of counterfeit goods from China comprised a slightly smaller percentage of all seizures of counterfeit goods made by U.S. Customs and Border Protection (CBP) and HSI, but this percentage change is related to the increase in seizures of counterfeit goods from other countries, not a decrease in seizures from China. China still accounts for nearly half (49 percent) of all seizures of counterfeit goods attempting to enter the United States.

ICE's HSI participates regularly in the U.S.-China Joint Liaison Group for Law Enforcement Cooperation (JLG), through our attaché offices in China. HSI also takes part in the JLG Intellectual Property Criminal Enforcement Working Group, led by the Department of Justice Computer Crime and Intellectual Property Section. An anecdotal assessment supports the conclusion that China responds more favorably to requests for assistance in investigations and prosecutions of foreign nationals that violate Chinese law

<b>Question#:</b>	11
<b>Topic:</b>	China
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	JUDICIARY (SENATE)

in China, as opposed to Chinese nationals engaging in criminal activity that violates the laws of the United States. HSI will continue to work through the JLG, and other vehicles, to increase IP theft enforcement cooperation with China, but with recognition that there has not been full cooperation so far.

While other federal agencies are heavily engaged in non-law enforcement efforts to decrease the importation of infringing goods from China, HSI continues to believe that the key three pillars for effective criminal IP theft enforcement between the United States and China are: training, information sharing, and joint operations. In this regard, HSI and the IPR Center, recently conducted a three day IPR Symposium funded by the Department of State, with participation from DOJ, USPTO, and CBP, in Hong Kong for representatives from Chinese, Hong Kong, Macanese, and Malaysian law enforcement and has future Department of State-funded training planned in the Philippines.

Current discussions with Chinese officials relating to IP theft enforcement tend to focus on the accomplishments made by China during their Special IPR Campaign that recently concluded. From October to December of 2010, during this campaign, China Customs advised HSI that it seized more than 2,000 shipments of counterfeit goods departing China with a value of more than \$18 million USD. These seizures included items that could pose a significant public safety risk, including counterfeit toothpaste, cigarettes, and electronics.

Unfortunately, U.S. law enforcement continues to encounter obstacles when attempting to obtain evidence for investigations or joint investigative efforts from the Chinese government in IP theft enforcement and several other important areas of U.S. national interest.

<b>Question#:</b>	12
<b>Topic:</b>	music sites
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Al Franken
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** In November 2010, several music sites had their domain names seized, including Dajaz1.com, OnSmash.com, RapGodFathers.com, and rmx4u.com. The site operator of OnSmash.com, a hip-hop music blog, has said the illegal music clips were given specifically to him by artists and record labels to generate publicity, and when asked, he always removed content. Other sites, like TVShack.net, host no illegal content, only link to infringing content. In all of these cases, the site operators did not receive notice prior to the domain name seizure, and they were given no opportunity to correct the infringement. By seizing an entire domain name, you are potentially disrupting access to both legal and illegal content.

Can you explain how ICE makes the decision to seize a domain name?

**Response:** ICE does not make decisions to seize domain names. That decision is made by a federal magistrate judge upon application under Section 2323 of Title 18 by ICE and attorneys with the Department of Justice. The application must be supported by an affidavit, signed and sworn to by an ICE Homeland Security Investigations' (HSI) agent. While there is not a minimum or maximum page length, many of the affidavits submitted for seizure of the domain names have regularly been dozens of pages long. One hundred and twenty five domains names have been seized during Operation In Our Sites, and in each of these cases, the seizure was preceded by a federal magistrate judge's determination that probable cause existed that the involved website was engaged in violations of federal copyright or trademark laws, resulting in issuance of federal seizure warrants. In addition to seizures of domain names, Operation In Our Sites has also resulted in seizure of approximately \$600,000 in cash from criminal as well as computer servers and other instrumentalities of criminal copyright and trademark violations. Two individuals have been charged criminally so far in U.S. District Court for the Southern District of New York.

All of the domain names seized through court orders obtained during Operation In Our Sites were commercial sites, profiting from criminal trademark violations and criminal copyright infringement, through a combination of sales, advertising revenue, and subscription fees. As a law enforcement agency, ICE has no interest in disrupting lawful commerce or protected speech. The targeted sites were designed with the specific intent to derive profits from other individuals' protected trademarked goods and copyrighted materials. Of the 125 domain names seized by ICE's HSI throughout Operation In Our Sites, almost 100 were engaged in the sale of counterfeit luxury goods, while the remaining sites illegally offered copyrighted first-run movies, music, and software.

<b>Question#:</b>	12
<b>Topic:</b>	music sites
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Al Franken
<b>Committee:</b>	JUDICIARY (SENATE)

Investigative leads for Operation In Our Sites come to HSI from various sources. These leads are run through established standard operating procedures for vetting and de-conflicting leads for potential domain name seizures and determining which domain names are targeted for seizure. This process, with multiple layers of oversight, takes several issues into account, including whether the sites significantly engage in illegal activity, whether HSI agents have purchased counterfeit merchandise from the site, and whether seizing the violative domain name will have an impact beyond the seizure itself.

During Operation In Our Sites, HSI special agents independently obtained counterfeit trademarked goods or pirated copyrighted material prior to applying for a federal seizure warrant based on probable cause. There were numerous layers of legal review throughout the process of obtaining a warrant, from supervisory agents within HSI, to Assistant U.S. Attorneys and trial attorneys within the Department of Justice (DOJ), and, ultimately the review by federal magistrate judges. As with all seizure warrants, the owners of the seized property have the opportunity to petition for a return of their property by challenging the judge's determination through a mandatory hearing. If the petition is filed, a hearing is held in a federal court to determine the validity of the affidavit supporting the seizure. In addition, the law provides several other vehicles by which a domain name owner can seek return of the domain name.

**Question:** Is there a way that ICE could more narrowly tailor blocking orders or verify intent and content prior to seeking a blocking order?

**Response:** ICE does not obtain "blocking orders" that deny access to websites. The order issued by a federal magistrate is a seizure warrant that instructs the domain name registry to redirect the violative domain name to a contract server retained by ICE's Homeland Security Investigations (HSI). The only content on the contract server is a seizure notice advising the owner of the domain name, and any visitors, that the domain name was seized pursuant to a court order issued by a U.S. District Court.

The criminal investigations undertaken by HSI and the Department of Justice (DOJ) must be incredibly thorough, because the law enforcement agencies bear the burden of showing, by probable cause, that the website is engaging in criminal copyright or criminal trademark violations. The criminal investigations include verification, prior to application for the seizure warrant, that the content, in a criminal copyright violation, was not authorized to be distributed through the particular website. In a trademark violation case, an HSI agent will purchase at least one and usually more counterfeit articles from the target website. If a petition is filed to return the domain name, ICE and DOJ would retain the burden at a full evidentiary hearing of proving the validity of the affidavit,

<b>Question#:</b>	12
<b>Topic:</b>	music sites
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Al Franken
<b>Committee:</b>	JUDICIARY (SENATE)

including whether the copyrighted content or trademarked goods were authorized for distribution on the website.

ICE cannot comment on the above noted domain name seizure because it is in litigation.

**Question:** Would a notice process which would allow domain operators to remove the illegal content prior to the domain name seizure be less effective or more difficult to implement?

**Response:** When Congress passed the *Prioritizing Resources and Organization for Intellectual Property Act of 2008* (“PRO IP Act”), it provided law enforcement with a civil forfeiture tool in Section 2323 of Title 18, for, *inter alia*, the forfeiture to the United States Government of “[a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense referred to [copyright infringement or trademark violations) . . . .” This provision, similar to other civil forfeiture provisions within the criminal code, is linked to the search and seizure provisions of the Federal Rules of Criminal Procedure and the forfeiture provisions of Title 18. These statutory provisions do not provide for “prior notice” before execution of a search and seizure warrant. Further, law enforcement agencies do not notify suspects of impending enforcement actions prior to their execution. Domain names are seized, through Operation In Our Sites, in furtherance of ongoing criminal investigations of violations of U.S. federal laws.



<b>Question#:</b>	13
<b>Topic:</b>	mooo.com
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Al Franken
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** In February 2011, ICE seized mooo.com as part of a child pornography investigation. This seizure redirected more than 84,000 sub domains to a warning that mooo.com had been seized for involvement with child pornography, despite the fact that the overwhelming majority of these sub domains only had legal content. ICE did fix what was later admitted to be an inadvertent mistake, but it took several days before the site was back up without the warnings displayed. What is ICE doing to make sure that other investigations that result in domain name seizures do not run into this sort of problem again?

**Response:** During a child pornography investigation involving websites offering graphic images of pre-pubescent children forced to engage in sexual acts, ICE, working with the Department of Justice, served a seizure warrant that was overly broad. This resulted in the seizure for 48 hours of domain names in addition to the intended target. Significantly, during that 48-hour period, over 1,000 individuals were prevented from visiting the site that contained the sexually exploitive images of children. However, the overly broad nature of the seizure warrant was not appropriate and, as noted in the question, ICE took the remedial action to restore all of the domain names associated with Mooo.com, except of course for the criminally violative one which had been removed by Mooo.com in the interim.

In subsequent investigations, ICE, working with DOJ, has instituted a significant site vetting process for domain names targeted for seizure and forfeiture. This process is memorialized in an IPR Center Standard Operating Procedure (SOP). This process contains multiple layers of oversight within the agency followed by numerous layers of legal review, throughout the process of obtaining a court-ordered seizure warrant, by Assistant U.S. Attorneys and trial attorneys from the Department of Justice, ultimately up to the federal magistrate judges. In a separate action, DOJ also sent out guidance to Assistant U.S. Attorneys that handle child pornography and intellectual property theft cases.

<b>Question#:</b>	14
<b>Topic:</b>	opinion
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** In your opinion, what has been the most successful aspect of the PRO-IP Act in achieving its goals of comprehensive intellectual property rights enforcement?

**Response:** The most successful aspect of the PRO-IP Act in achieving its goals of comprehensive intellectual property rights enforcement has been the seizure and civil forfeiture provision provided to law enforcement. This provision has facilitated the ability of law enforcement to prevent entities and/or persons from profiting from the commission of intellectual property theft and allowing seizures of instrumentalities of IP theft.

<b>Question#:</b>	15
<b>Topic:</b>	challenge
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** In your opinion, what is the greatest challenge that ICE faces with respect to IP enforcement? What is the greatest challenge that we face with respect to IP theft?

**Response:** While globalization provides boundless opportunities for commerce, it also brings a growing set of challenges, especially in combating the theft of intellectual property (IP).

The Internet has now become the primary vehicle through which to market, distribute, and sell counterfeit or copyrighted items illegally, making IP theft enforcement much more complex and challenging. The Internet enables criminal enterprises to sell counterfeit goods directly to customers around the world, often times while appearing legitimate. Offenders create websites that appear similar to the rights holder's own websites, potentially deceiving consumers into purchasing counterfeit goods. In recent years, the supply for counterfeit goods has shifted from the lower profit secondary market, where consumers know they are purchasing counterfeit goods, to the primary market, a marketplace in which consumers are not as capable of determining whether they are purchasing genuine goods. The price points of counterfeit goods sold over the Internet are not always so low that a consumer should have the requisite indicators that the product is counterfeit.

There are many challenges to combating Internet-based crime. It is often difficult to identify and locate foreign website operators. When the foreign website operators are located, foreign government cooperation is required to obtain successful prosecution. This is why domain name seizure is sometimes the best option U.S. law enforcement has to enforce federal criminal copyright and trademark laws.

ICE's Homeland Security Investigations (HSI) is also working on increasing public awareness of IP violations through enforcement actions, press releases, and public service announcements. ICE meets with Internet advertising associations and various Internet and online payment providers to discuss ways to fight IP crimes committed over the Internet and we participate in the IPEC's stakeholders meetings on these issues. The National Intellectual Property Rights Coordination Center is working with its agency partners and with industry on a number of different initiatives related to public messaging.

<b>Question#:</b>	16
<b>Topic:</b>	penalties
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** The PRO-IP Act increased penalties for certain intellectual property crimes. How effective have stricter penalties been in deterring intellectual property rights violations? What effect have they had on enforcement?

**Response:** U.S. Immigration and Customs Enforcement defers to the Department of Justice on the effectiveness of stricter penalties in deterring intellectual property rights.

<b>Question#:</b>	17
<b>Topic:</b>	trends
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** What kinds of trends are you seeing with respect to intellectual property theft, piracy and counterfeiting? Are we able to keep up with the evolving methods and technologies utilized by IP criminals? Are the laws on the books able to keep up with the criminals?

**Response:** Historically, counterfeit goods were smuggled into the U.S. in bulk shipments utilizing sea containers and were typically sold at storefronts or by street vendors. Criminal organizations involved in intellectual property (IP) theft are now increasingly using the Internet to distribute their goods and content. Foreign-based IP smuggling organizations are also shifting their shipping methods to express consignment couriers and mail services to send smaller amounts of their products directly to purchasers.

ICE's Homeland Security Investigations (HSI) has adapted to the evolving distribution and shipping methods used by criminals by targeting illicit Internet-based companies and working closely with U.S. Customs and Border Protection at seaports, mail facilities, and express consignment centers. As an example, HSI initiated Operation In Our Sites in June 2010, targeting websites used in violation of federal criminal copyright and trademark laws. Through Operation In Our Sites, HSI has seized 125 domain names of websites actively engaged in counterfeiting or copyright violations.

In addition, the HSI-led National Intellectual Property Rights Coordination Center works closely with industry, government, and the public to further educate them on counterfeit goods and associated laws. In FY 2010, HSI conducted 225 outreach events with 14,684 participants. For FY 2011 to date, ICE has conducted 162 events with 7,844 participants.

ICE has worked closely with its U.S. Government counterparts and the Intellectual Property Enforcement Coordinator on the Administration's White Paper on IP Enforcement Legislative Recommendations. ICE strongly supports the recommendations in this document to increase penalties and enhance legislation to strengthen IP theft enforcement.

<b>Question#:</b>	18
<b>Topic:</b>	input
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** Walk us through the specific methods that the IPR Center uses to get input from its partners. How many more members are you hoping to add to the IPR Center?

**Response:** The National Intellectual Property Rights Coordination Center (IPR Center) currently has 19 partners. The IPR Center Principals, which include senior management from each partner agency, meet regularly to discuss issues relevant to the center and the addition of potential new partner agencies. Any agency with an intellectual property mission is invited to attend and petition to join the IPR Center or contribute to its mission.

In addition, the IPR Center receives input from all of the IPR Center partners through weekly led dissemination and case de-confliction meetings. Investigative case referrals and leads to IPR Center partner agencies are researched and reviewed by all partners through a process called de-confliction. When leads are received directly by the IPR Center, intelligence reports are first generated from those leads as part of the vetting process. Leads and case referrals from partner agencies are distributed to all partner agencies and the Department of Justice Computer Crimes and Intellectual Property Section for vetting and de-confliction to determine whether an agency is already investigating the alleged IP violation. At the weekly de-confliction meeting, IPR Center partners review the results of this de-confliction process and establish which partner agency or agencies will be responsible for determining future action on that lead. The lead partner agency then coordinates with the IPR Center to ensure any further enforcement action is tracked, monitored, de-conflicted, and reported to IPR Center partners.

<b>Question#:</b>	19
<b>Topic:</b>	CCIPS
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** What can improve the IPR Center's efficiency and cooperation? Would it improve the effectiveness of the IPR Center if CCIPS were a partner?

**Response:** Many of the National Intellectual Property Rights Coordination Center (IPR Center) partners are assigned to the IPR Center as a collateral duty, based upon personnel and budgetary issues. They attend the scheduled de-confliction meetings and further communicate via emails and phone, but are not at the IPR Center on a daily basis. Having partners at the IPR Center on a regular basis would further enhance the efficiency and cooperation of the IPR Center. Although not a formal partner, the Department of Justice Computer Crime and Intellectual Property Section (CCIPS) is an active participant at the IPR Center. CCIPS personnel attend the weekly de-confliction meetings. CCIPS regularly attends IPR Center meetings including operational strategy meetings, meetings concerning ongoing operations or investigations, and those with private industry.

<b>Question#:</b>	20
<b>Topic:</b>	seizures
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** Has ICE been the subject of any civil legal action as a result of its seizures in Operation In Our Sites or other counterfeit goods seizures?

**Response:** There are several pending civil actions resulting from the seizure of domain names through Operation In Our Sites. ICE defers to the Department of Justice for further information.



<b>Question#:</b>	21
<b>Topic:</b>	memorandum
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

**Question:** ICE recently signed a Memorandum of Understanding with the Chinese government, has two offices in China, and is engaged in significant enforcement work in Shenzhen. What else is ICE doing to obtain increased cooperation in IPR enforcement from the Chinese government?

**Response:** In addition to the actions mentioned in the question above, U.S. Immigration and Customs Enforcement (ICE) has taken a proactive approach to increase cooperation with the Chinese Government on intellectual property (IP) theft enforcement focusing upon senior level engagement, information exchange, and training.

On September 14, 2010, Director Morton met with Chinese Ministry of Public Security (MPS) Director General Meng Qing-Fing and signed an agreement for greater cooperation between the two agencies to combat intellectual property crime and money laundering. The agreement is historic and shows progress in a sustained effort to secure MPS cooperation on cases of mutual concern. The signing of the agreement resulted in an unplanned meeting between Director Morton and MPS Vice Minister Meng Hongwei. Embassy representatives were encouraged by the level of agreement to exchange investigative information, as previously such information sharing had been entirely ad hoc. Chinese law enforcement officials agreed to exchange information, engage in joint intellectual property investigations, and meet regularly at the highest levels. ICE would like to see more timely cooperation and joint investigations, which so far have not been readily apparent.

ICE participates regularly in the U.S.-China Joint Liaison Group for Law Enforcement Cooperation (JLG). ICE takes part in the JLG Intellectual Property Criminal Enforcement Working Group, which is led by the Department of Justice Computer Crime and Intellectual Property Section. China favors investigations and prosecutions of foreign nationals that violate Chinese law in China; as such, during the November 2010 meeting, U.S. law enforcement members of the JLG proposed three joint investigations involving ICE targets in China. Activity on these investigations is ongoing. ICE will continue to work through the JLG to increase IP theft enforcement cooperation with China.

Through the assistant attaché in Guangzhou, ICE has agreed to provide MPS with data about CBP seizures with a nexus to China and with actionable information from ICE investigations and operations in order to further investigations in both countries. ICE has already provided such information to China and will continue to do so.

<b>Question#:</b>	21
<b>Topic:</b>	memorandum
<b>Hearing:</b>	Oversight of Intellectual Property Law Enforcement Efforts
<b>Primary:</b>	The Honorable Charles E. Grassley
<b>Committee:</b>	JUDICIARY (SENATE)

The MPS in China requested help from the ICE Attaché in Beijing related to the transnational distribution and smuggling of counterfeit cigarettes by a U.S. citizen. On August 26, 2010, acting on information provided by MPS, U.S. Customs and Border Protection in Long Beach seized 19,804 cartons of Chinese brand cigarettes with an MSRP value of \$1.5 million. Two defendants were tried recently in China, and on December 8, 2010, the U.S. citizen was sentenced by Chinese authorities to 16 years incarceration for criminal violations related to the manufacture and distribution of counterfeit goods, and prior criminal violations related to vehicle smuggling. The other defendant, a Chinese national, was sentenced to three years' incarceration for criminal violations related to the manufacturing and distribution of counterfeit goods.

ICE has worked with other U.S. Government partners to provide training to Chinese government officials jointly with other government officials in Asia in order to better enhance collaboration. The ICE Office of Homeland Security Investigations Southeast Asia IPR Criminal Enforcement Symposium was held in Hong Kong from May 24-27, 2011. IP Attaché Guangzhou coordinated the participation of 28 officials from Mainland China, including representatives from the Ministry of Public Security, the General Administration for China Customs, and the Supreme People's Procuratorate Office. Other law enforcement participants in the symposium included representatives from Malaysia, Hong Kong, and Macau.

HSI Attaché Beijing is working with the U.S. Embassy on an IPR Symposium that will be co-hosted by Chinese and Japanese officials in Qingdao, China on September 7-9, 2011. If this symposium occurs, this will be the first time IPR Center training will be held in mainland China.

Additionally, ICE has been aggressively reaching out to U.S.-based businesses operating or manufacturing in China to inquire about their IPR problems and educate them on some of the legal issues they need to be aware of to protect their IPR when operating in China. Some companies ICE has spoken to have been unable to get responses from Chinese officials when they have IPR issues. ICE has subsequently learned that some of these companies have never actually registered their patents or trademarks with China, leaving them with no protection at all from infringers.

RESPONSES OF JASON M. WEINSTEIN TO QUESTIONS SUBMITTED BY SENATORS  
COBURN, FRANKEN, AND HATCH

(Note: At the time of printing, after several attempts to obtain responses to the written questions, the Committee had not received any communication from the witness.)

## MISCELLANEOUS SUBMISSIONS FOR THE RECORD

AMERICAN FEDERATION OF MUSICIANS, AMERICAN FEDERATION OF TELEVISION AND RADIO ARTISTS, DIRECTORS GUILD OF AMERICA, INTERNATIONAL ALLIANCE OF THEATRICAL STAGE EMPLOYEES, MOVING PICTURE TECHNICIANS, ARTISTS AND ALLIED CRAFTS OF THE UNITED STATES, ITS TERRITORIES AND CANADA, INTERNATIONAL BROTHERHOOD OF TEAMSTERS, SCREEN ACTORS GUILD, JUNE 20, 2011, JOINT LETTER



June 20, 2011

The Honorable Patrick J. Leahy  
Chairman, Committee on the Judiciary  
SR-433 Russell Senate Office Building  
Washington, DC 20510

The Honorable Chuck Grassley  
Ranking Member, Committee on the Judiciary  
SH-135 Hart Senate Office Building  
Washington, DC 20510

Dear Chairman Leahy and Senator Grassley:

On behalf of the American Federation of Musicians, American Federation of Television and Radio Artists, Directors Guild of America, International Alliance of Theatrical Stage Employees, International Brotherhood of Teamsters, and Screen Actors Guild; we would like to express our great appreciation of, and support for, the attention and resources that the Department of Homeland Security continues to expend on the fight against digital theft.

Specifically, we want you to know that we believe that ICE's "Operation In Our Sites" is an invaluable bulwark—not just for us, but for American consumers against the proliferation of profit-making websites that are dedicated to selling counterfeit goods, stolen films, TV shows, and music. "Operation In Our Sites" has created much greater public recognition of the problem and demonstrated to businesses relying on infringement and counterfeiting that they may no longer act with impunity on a lawless Internet.

Together, our organizations represent 400,000 working men and women who are involved in the creation of a variety of motion pictures, television programs and sound recordings that entertain and educate consumers around the world. Protection of our members' ability to earn a living from the sale and distribution of that content is our major priority. In 2010 alone downstream revenues from the reuse of feature films and television programs and lawful sales of sound recordings generated \$1.5 billion in essential residuals and royalties for the members of AFTRA, DGA, IATSE, and SAG. Additionally, these residuals and royalties also play a significant role in funding the health and pension plans that benefit all of our members—for example they constitute 60% of the Motion Picture Industry Health Plan for IATSE members.

Because it is these "downstream" sales (such as DVDs, pay-per-view) that are most vulnerable and most severely impacted by digital theft; our members feel the pain from both the corrosive effect on reinvestment and erosion that piracy has on residuals and royalties. This is why we expressed our unqualified support for this effort when "Operation In Our Sites" was first launched and why we do so again.

In response to pressure put on criminal business operators by "Operation In Our Sites", many have fled to web domains in countries that have little respect for the intellectual property of U.S. creators. Currently, they are able to circumvent U.S. law enforcement and continue their criminal enterprises to the detriment of the men and women we represent. We support pending legislation that would give additional tools to law enforcement to combat these criminal operators that are currently beyond the reach of U.S. law enforcement.

Thank you for your continued efforts to protect the jobs and livelihoods of our members; and for your on-going work to protect our economy from looting by criminal enterprises.

Sincerely,

American Federation of Musicians (AFM)  
American Federation of Television and Radio Artists (AFTRA)  
Directors Guild of America (DGA)  
International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists and Allied Crafts of the United States, Its Territories and Canada (IATSE)  
International Brotherhood of Teamsters (IBT)  
Screen Actors Guild (SAG)

AMERICAN SOCIETY OF COMPOSERS, AUTHORS, AND PUBLISHERS (ASCAP), PAUL WILLIAMS, PRESIDENT AND CHAIRMAN OF THE BOARD, NEW YORK, NEW YORK, JUNE 20, 2011, LETTER



PAUL WILLIAMS  
President and  
Chairman of the Board

June 20, 2011

The Honorable Patrick J. Leahy  
Ranking Member, Senate Committee on the Judiciary  
152 Dirksen Senate Office Building  
Washington DC 20510

The Honorable Chuck Grassley  
Chairman, Senate Committee on the Judiciary  
224 Dirksen Senate Office Building  
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Grassley:

I write on behalf of the American Society of Composers, Authors, and Publishers (ASCAP) with regard to the upcoming, June 22 Senate Judiciary Committee hearing on "Oversight of U.S. Intellectual Property Law Enforcement Efforts." ASCAP believes that all of our law enforcement agencies deserve commendation for their continued efforts to protect the rights of American creators, including the over 410,000 songwriters, composers, and publishers we represent. Unquestionably, these rights and their enforcement make a valuable contribution to a strong American economy. ASCAP's songwriters and composers are the smallest of small business people generating many layers of jobs across multiple industries as their creative output is extended to the public. And, the positive balance of trade resulting from their efforts is significant.

For all these reasons, ASCAP respectfully requests that you include this letter in the hearing record so that our appreciation for the hard work and dedication of our law enforcement agencies is known to all.

Deserving special recognition at this point in time is the U.S. Immigration and Custom Enforcement (ICE) agency within the Department of Homeland Security. A little over a year ago, ICE began its innovative IP enforcement effort, "Operation in Our Sites." Since that time, "Operation in Our Sites" has experienced unparalleled success in shuttering over one hundred websites that trafficked in a wide range of stolen U.S. intellectual property. Of even more importance, ICE has steadfastly pursued this initiative despite the usual, tired criticism from piracy apologists and profiteers. In doing so, ICE sends a clear, much-needed message to

AMERICAN SOCIETY OF COMPOSERS, AUTHORS & PUBLISHERS  
ASCAP Building, One Lincoln Plaza, New York, New York 10023  
212.621.6201 Fax: 212.721.0955  
7920 West Sunset Boulevard, Third Floor, Los Angeles, CA 90046  
323.883.1000 Fax: 323.883.1049  
E-Mail: [pwilliams@ascap.com](mailto:pwilliams@ascap.com)  
<http://www.ascap.com>

thieves and America's creators alike: law enforcement is committed to stopping the online looting of American creativity and ingenuity. As an American music creator, and a representative of over 410,000 other such creators at ASCAP, I can tell you that we greatly appreciate the work that our government is doing to protect us.

Respectfully,

A handwritten signature in black ink, appearing to read "Paul Williams". The signature is fluid and cursive, with a large initial "P" and a long, sweeping underline.

Paul Williams  
President and Chairman of the Board  
ASCAP

INSTITUTE FOR POLICY INNOVATION (IPI), TOME GIOVANETTI, PRESIDENT,  
LEWISVILLE, TEXAS, JUNE 20, 2011, LETTER



June 20, 2011

Senator Patrick J. Leahy  
Chairman

Senator Chuck Grassley  
Ranking Member

Senate Judiciary Committee

Dear Senators Leahy and Grassley:

The Institute for Policy Innovation (IPI) commends to you and to your colleagues on the committee the important work of U.S. Immigration and Customs Enforcement in working to reduce the harmful impact of piracy and counterfeiting on the U.S. economy.

IPI works actively in the area of intellectual property policy, and is an accredited observer NGO with the World Intellectual Property Organization (WIPO). Our research has helped to document the harm done to the U.S. economy by piracy and counterfeiting, and IPI believes that strong IP protection and enforcement is critical to the vitality and global competitiveness of the U.S. economy.

We are aware of the efforts of ICE through a personal briefing we were given at the National Intellectual Property Rights Coordination Center, though the regular email updates that we receive, and through the testimony of other agencies that work in coordination with ICE; specifically, of ICE's operations related to Internet websites distributing pirated and counterfeit goods, and the success of their surge enforcement operations against distributors of such goods.

In an economy that is increasingly dependent on our ability to create and innovate, and to export those goods worldwide, it is vital that American workers have their livelihoods protected from piracy and counterfeiting, and that American consumers be protected from the harm of illegal goods.

We sincerely appreciate the efforts of ICE, and of the Judiciary Committee, and pledge to assist you in any way that we can to ensure the vitality of the U.S. economy through strong IP enforcement.

Sincerely,

Tom Giovanetti  
President

[www.ipi.org](http://www.ipi.org)

Tom Giovanetti  
President  
[tomg@ipi.org](mailto:tomg@ipi.org)

**Board of Directors**

Chairman  
Michael E. Williams, Ph.D.  
University of Texas

Mark Miller

Roger E. Meiners, Ph.D.  
Professor of Law and Economics  
University of Texas at Arlington

Ryan C. Amacher, Ph.D.  
Professor of Economics and Public Affairs  
University of Texas at Arlington

**Board of Advisors**

Ernest S. Christian  
Chief of Strategy, Tax Rights

Stephen J. Ekin  
President and Executive Director  
Institute for Research on the Economics of Taxation

James Olan Hutchinson  
President  
Sagebrush Forum

Stephen Moore  
Editorial Board  
Wall Street Journal

Gregory Tullock  
Professor of Law and Economics  
George Mason University

James R. Von Ehr, II  
President and CEO  
Zyme

Thomas G. West  
Professor of Public  
University of Dallas

1669 South Stemmons,  
Suite 245  
Lewisville, TX 75067  
(972) 874-5139 voice  
(972) 874-5144 fax

[email ipi@ipi.org](mailto:email ipi@ipi.org)

COLLEEN M. KELLEY, NATIONAL PRESIDENT, NATIONAL TREASURY EMPLOYEES  
UNION, (NTEU), WASHINGTON, DC, STATEMENT



**STATEMENT OF COLLEEN M. KELLEY  
NATIONAL PRESIDENT  
NATIONAL TREASURY EMPLOYEES UNION**

**ON**

**INTELLECTUAL PROPERTY  
LAW ENFORCEMENT**

**BEFORE THE**

**COMMITTEE ON THE JUDICIARY  
UNITED STATES SENATE**

**June 22, 2011**



Chairman Leahy, Ranking Member Grassley, distinguished members of the Committee, thank you for the opportunity to provide this testimony. As President of the National Treasury Employees Union (NTEU), I have the honor of leading a union that represents over 24,000 Customs and Border Protection (CBP) Officers, Agriculture Specialists and trade enforcement and compliance specialists who are stationed at 331 land, sea and air ports of entry across the United States.

**Customs and Border Protection Entry Specialists, Import Specialists, Paralegal Specialists that determines fines, penalties and forfeitures, Customs Auditors and Attorneys and other trade compliance personnel are the frontline of defense against illegal imports and contraband. These employees enforce over 400 U.S. trade and tariff laws and regulations in order to ensure a fair and competitive trade environment pursuant to existing international agreements and treaties, as well as stemming the flow of illegal imports, such as pirated intellectual property and counterfeit goods, and contraband such as child pornography, illegal arms, weapons of mass destruction and laundered money.**

**Along with facilitating legitimate trade and enforcing trade and security laws, CBP trade personnel are responsible for stopping illegal transshipments, goods with falsified country of origin, goods that are misclassified and for collecting antidumping and countervailing duties. CBP is also a revenue collection agency—collecting \$32 billion in duties and fees on imports valued at more than \$2 trillion in 2007.**

#### **TRADE ENFORCEMENT AND COMPLIANCE STAFFING**

When CBP was created, it was given a dual mission of not only safeguarding our nation's borders and ports from terrorist attacks, but also the mission of regulating and facilitating international trade. CBP is responsible for collecting import duties and ensuring importers fully comply with applicable laws, **including statutes enforcing intellectual property rights (IPR)**, trade regulations, quotas, and Free Trade Agreement (FTA) requirements.

Customs revenues are the second largest source of federal revenues collected by the U.S. Government after tax revenues. This revenue funds other federal priority programs. NTEU is deeply concerned with the lack of resources, both in dollars and manpower, devoted to CBP's trade functions. Lack of sufficient focus and resources costs the U.S. Treasury in terms of customs duties and revenue loss and costs American companies in terms of lost business to unlawful imports.

Because of continuing staffing shortages, inequitable compensation, and lack of mission focus, experienced CBP commercial operations professionals at all levels, who long have made the system work, are leaving or have left the agency. Twenty-five percent of CBP Import Specialists will retire or be eligible to retire within the next few years.

When Congress created the Department of Homeland Security, the House Ways and Means and Senate Finance Committees included Section 412(b) in the Homeland Security Act (HSA) of 2002 (P.L. 107-296). This section mandates that "the Secretary [of Homeland Security] may not consolidate, discontinue, or diminish those functions...performed by the

United States Customs Service...on or after the effective date of this Act, reduce the staffing level, or reduce the resources attributable to such functions, and the Secretary shall ensure that an appropriate management structure is implemented to carry out such functions.”

In October 2006, Congress enacted the Security and Accountability For Every (SAFE) Port Act (P.L. 109-347.) Section 401(b)(4) of the SAFE Port Act directed the DHS Secretary to ensure that requirements of section 412(b) of the HSA (6 U.S.C. 212(b)) are fully satisfied.

CBP satisfied this statutory requirement by freezing the number of many maintenance of revenue function positions at the level in effect on the date of creation of the agency in March 2003. As you know, CBP was created by the merger of the former U.S. Customs Service, the Immigration and Naturalization Service, and the Animal, Plant, Health Inspection Service. In March 2003, the number of commercial operations employees at the former U.S. Customs Service was significantly less than prior to 9/11 and significantly less than the need as stated in the U.S. Customs Service Optimal Staffing Levels Fiscal Years 2000-2002 (February 25, 2000), known as the Resource Allocation Model (RAM).

For example, according to the U.S. Customs RAM, in FY 1998, the optimal staffing level for Import Specialists at the U.S. Customs Service was 1,249 and, based on workload in FY 2002, the optimal staffing level for Import Specialists was 1,489 (pages 2, A-1 and M-1 through M-12.) In actuality, in March of 2003 when CBP stood up, there were only 984 Import Specialists on-board. That is 265 Import Specialist positions less than the 1998 base total, and 505 less than the FY 2002 Import Specialists optimal staffing level. A significant reduction in the number of revenue maintenance function positions had occurred at the U.S. Customs Service between 9/11 and March 2003 when CBP stood up. Section 412(b) of the HSA reflected Congress’ concern regarding this diminishment in the number of customs revenue function positions versus customs security function positions at the U.S. Customs Service and fear that it would continue and be exacerbated by its merger into CBP.

Even though CBP complied with the letter of Section 401 (b)(4) of the SAFE Port Act, it appears to NTEU that CBP views the “March FY 2003 Staff On-Board” numbers of revenue maintenance function positions (see Appendix I), including such vital trade facilitation and enforcement positions as Entry and Import Specialists, as a ceiling rather than a floor.

#### **CBP’s Resource Allocation/Optimization Model**

CBP’s adherence to the March 2003 Import Specialist employment number as a ceiling has become evident in the most recent iteration of the SAFE Port Act mandated Resource Allocation Model. **Section 403 of the SAFE Port Act required CBP to complete a Resource Allocation Model (RAM) by June 2007, and every 2 years thereafter, to determine optimal staffing for commercial and revenue functions.** It directed that the model must comply with the requirements of section 412(b) of the Homeland Security Act (HSA) of 2002 and required the CBP Commissioner, not later than September 30, 2007, to ensure that the requirements of 412(b) of the HSA were fully satisfied. The CBP positions covered by Section 412(b) include “Import Specialists, Entry Specialists, Drawback Specialists, National Import Specialists, Fines

and Penalty Specialists, Attorneys at the Office of Regulations and Rulings, Customs Auditors, International Trade Specialists, and Financial Systems Specialists.”

The rationale for this provision arose from a Government Accountability Office (GAO) report (GAO-05-663) that stated, “as of June 2003, CBP has not increased staffing levels [at the ports of entry]” and “CBP does not systematically assess the number of staff required to accomplish its mission at ports and airports nationwide...” Further, GAO observed that “not identifying optimal staffing levels prevents CBP from performing workforce gap analyses, which could be used to justify budget and staffing requests.”

The former U.S. Customs Service’s last internal review of staffing for Fiscal Years 2000-2002, dated February 25, 2000, shows that the U.S. Customs Service needed over 14,776 new hires just to fulfill its basic mission (U.S. Customs RAM, page 2 and A-1)--and that was before 9/11. Since then, the Department of Homeland Security was created and the U.S. Customs Service was merged with the Immigration and Nationalization Service and parts of the Agriculture Plant Health Inspection Service to create CBP. CBP was given an expanded mission of providing for both the first line of defense against domestic terrorism and making sure trade laws are enforced and trade revenue collected.

The first SAFE Port Act Section 403 RAM, dated July 6, 2007, stated that “CBP has over 8,200 employees that are involved in commercial trade operations. The Model suggests that to carry out these commercial operations and to adequately staff the needs for priority trade functions, the optimal level of staff in FY 2008 would be over 10,000 employees” (See CBP Report to Congress on Trade Resource Allocation Model, page 12.) According to the 2007 RAM, 1,100 Import Specialists would be needed for optimal performance in FY 2010, an increase of 116 over the HSA Floor (see CBP Report to Congress on Trade Resource Allocation Model, page 16).

In 2009, CBP renamed the SAFE Port Act Section 403 Resource Allocation Model (RAM). It is now called the Resource Optimization Model (ROM). The FY 2009 ROM reduces the FY 2010 optimal staffing levels for some revenue maintenance function positions, specifically the Entry and Import Specialist positions (see Appendix II). For example, the FY 2009 ROM puts the number of Import Specialist positions needed in FY 2010 at the HSA floor number of 984, rather than 1,100 as stated in the FY 2007 RAM.

#### **Fines Penalties and Forfeitures Staffing and IPR Seizures**

There is also a staffing crisis developing in CBP’s Fines Penalties and Forfeitures (FP & F) section, whose staff is responsible for resolving IPR seizures. **According to CBP’s 2009 Resource Optimization Model (see Appendix II), CBP should have had 514 FP&F Officers and Paralegal Specialists on the board by 2010. Full time permanent staffing numbers, however, provided to NTEU by CBP show that, as of March 12, 2011, there are only 315 FP & F Officers and Paralegal Specialists on board--36 GS-930 FP&F Officers and 279 GS-950 Paralegal Specialists (a number that includes but is not limited to FP&F Specialists)—a shortage of 200 positions.**

CBP Officers and Import Specialists have both been tasked with increasing the number of IPR shipments that are reviewed and seized. This has resulted in an unprecedented number of IPR seizure cases. **FP & F and Paralegal Specialists are responsible for processing these seizure cases. Because of due process requirements under the Fourth Amendment, CBP is required to process these cases in a timely fashion. Unfortunately, because of FP & F and Paralegal Specialists staffing shortages, CBP cannot always meet these timelines, and importers are able to move their shipments into commerce, rather than have IPR violative goods forfeited and destroyed.**

According to CBP's own Resource Optimization Model, CBP has a critical shortage in FP&F and Paralegal Specialists and is not taking needed action to fill these positions. **With ever increasing IPR seizures, this will necessarily result in due process releases. CBP cannot make the case that they are enforcing the law when counterfeit shipments are being released instead of destroyed.**

#### **FY 2012 CBP Budget Request**

Several years ago, pursuant to the provisions of the SAFE Port Act, there was a small increase in the number of CBP trade enforcement and compliance personnel. There was no increase in funding for CBP trade operations staffing, however, in the FY 2010 DHS appropriations bill or in the FY 2011 Continuing Resolution.

In effect, there has been a virtual CBP trade staffing freeze at March 2003 levels and, as a result, CBP's revenue function has suffered. **The FY 2012 budget requests funding for CBP's enforcement program to "prevent trade in counterfeit and pirated goods, and enforce exclusion orders on patent-infringing and other Intellectual Property Rights violative goods."** This request, however, includes no increase in CBP trade operations staff at the ports of entry to implement this trade enforcement program. NTEU urges the Committee to support funding to hire additional trade enforcement and compliance personnel, including FP & F and Paralegal Specialists, at the ports of entry to enforce trade laws.

#### **CBP Career Ladder Pay Increase**

NTEU commends the Department for the recent increase in journeyman pay for CBP Officers and Agriculture Specialists. Unfortunately, many deserving CBP trade and security positions were left out of this pay increase, which has significantly damaged morale. The 23,450 armed, uniformed CBP Officers and uniformed CBP Agriculture Specialist will be eligible for the increase, but the approximately 2,000 non-uniformed CBP commercial operations employees will not.

**NTEU strongly supports extending this same career ladder increase, from GS-11 to GS-12, to additional CBP positions, including CBP Entry, Import and Paralegal Specialists and CBP Seized Property Specialists. The journeyman pay level for the CBP Technicians who perform important commercial trade and administrative duties should also be increased from GS-7 to GS-9.** These upgrades are long overdue and would show CBP trade personnel that Congress recognizes the high level of expertise that these employees possess.

**Conclusion**

Customs revenues are the second largest source of federal revenues that are collected by the U.S. Government. Congress depends on this revenue source to fund priority programs. The Committee should be concerned as to how much CBP trade enforcement staffing shortages cost in terms of revenue loss to the U.S. Treasury.

**NTEU urges the Committee to support the hiring of additional needed CBP trade staff to enforce the over 400 U.S. trade and tariff laws and regulations, including IPR, for which they are responsible.**

The more than 24,000 CBP employees represented by the NTEU are proud of their part in keeping our country free from terrorism, our neighborhoods safe from drugs and our economy safe from illegal trade.

Thank you for the opportunity to submit this testimony on their behalf.

## Appendix I

**U.S. CUSTOMS AND BORDER PROTECTION**  
**REVENUE FUNCTIONS IDENTIFIED IN THE HOMELAND SECURITY ACT (HSA)**

Original Revenue Positions cited in Section 412

<u>Revenue Function</u>	<u>BASELINE</u>		<u>Current March 2006</u>	
	<u>March FY 2003 Staff On-Board</u>	<u>March FY 2003 Cost</u>	<u>March FY 2006 Staff On-Board</u>	<u>March FY 2006 Cost</u>
Import Specialist	984	\$72,920,503	892	\$84,715,650
			Future Hires - 111	
Entry Specialist	409	28,217,005	408	36,617,416
			Future Hires - 45	
Drawback Specialist	37	2,850,599	31	3,248,643
			Future Hires - 6	
National Import Specialist	97	9,478,537	87	10,895,376
			Future Hires - 10	
Fine Penalty & Forfeiture Specialist	203	14,580,495	218	20,194,672
Attorney's - Office of Regulations and Rulings	90	8,980,271	85	10,699,972
			Future Hires - 5	
Customs Auditor	364	31,726,698	351	37,541,977
			Future Hires - 16	
International Trade Specialist	74	7,577,977	62	7,721,266
			Future Hires - 12	
Financial Systems Specialists and Other Misc. Specialists	5	491,169	9	1,053,873

Other trade, cargo and commercial activities

In addition to the specific revenue positions cited above, there are many other aspects of CBP, involving government and contractor personnel, that work in the trade, cargo and commercial environment described in Section 415 of the HSA, such as:

- CBP officers working in Free and Secure Trade (FAST) enrollment and processing centers to facilitate entry of commercial goods into the U.S.;
- Mail specialists processing mail to ensure proper collection of duties;
- An estimated 5,800 CBP officers screening, inspecting and processing cargo at sea, air and land ports of entry;
- IT specialists, client representatives and contractor personnel supporting ACS and ACB systems, which process the collection of customs duties, process cargo with respect to the assessment and collection of duties, enforce quotas, and collect import data;
- Laboratory scientists classifying merchandise for purposes of compliance with all applicable customs and trade provisions;
- Finance personnel and contractors supporting CBP bond and Continued Dumping Subsidy Offset Act responsibilities.

Note: Future hires represent hiring to backfill attrited positions and/or new hires.

## Appendix II

CBP Report to Congress  
2009 ROM - 2006 SafePorts Act

Position Involved	Function	HSA Floor	FY08 (9.30.08)	FY08 (TRADE)	FY10	+/-, FY08 Trade to FY10	Future Projected Needs
							range: from 1 to 2
1 Agriculture Specialist	OFO	N/A	2,276	1,366	1,550	184	1,581
2 CBP Officer (Cargo)	OFO	N/A	19,518	4,880	4,678	(202)	4,792
3 Chemist	OT	N/A	101	101	129	28	137
4 Customs Attorney	OR&R	90	90	90	95	5	103
5 Customs Auditor	OT	364	364	364	459	95	479
6 Drawback Specialist	OFO	37	40	40	42	2	43
7 Entry Specialist	OFO	409	455	455	359	(96)	359
8 Financial Systems Specialist	HQ	5	1	5	6	1	6
9 FP&F Specialist	OT	203	237	128	514	386	519
10 Import Specialist	OFO	984	986	986	984	(12)	975
11 International Trade Specialist	OT	74	132	132	188	86	203
12 National Account Manager	OT	N/A	41	41	79	38	80
13 National Import Specialist	OT	97	101	101	101	0	104
14 Seized Property Specialist	OT	N/A	135	80	89	19	99
Total		2,253	24,457	8,779	9,293	(310)	9,480
15 CBP Tech			985	483	1,097		1,111
	OFO (124)						
	OT 632						
	Oth 6						
	Tr 514						
Analytical Support Ratio (15:1)					54		56
Admin Support Ratio (15:1)					542		544
Total					10,986	(310)	11,191
							11,805

MOTION PICTURE ASSOCIATION OF AMERICA, INC., PARAMOUNT PICTURES CORPORATION, SONY PICTURES ENTERTAINMENT INC., TWENTIETH CENTURY FOX FILM CORPORATION, UNIVERSAL CITY STUDIOS LLC, WALT DISNEY STUDIOS MOTION PICTURES, WARNER BROS. ENTERTAINMENT INC., JUNE 22, 2011, JOINT LETTER



June 22, 2011

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

The Honorable Charles Grassley  
Ranking Member  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Grassley:

We write to thank you for holding a hearing entitled "Oversight of Intellectual Property Law Enforcement Efforts." The Committee has always been a champion of America's copyright community and there is no more important time than now to review and conduct oversight of law enforcement's efforts to combat the theft of American creative works.

As you know, the U.S. intellectual property (IP) industries are critical to the health of our economy. Our industry alone produces billions of dollars in tax revenues each year, consistently generates a positive balance of trade with every country in the world, and is contributing to the economic recovery in areas hard-hit by recession. Millions of middle-class Americans go to work each day to make and sell the products that depend on copyright protection, from blockbuster films and award-winning television shows to life-saving pharmaceuticals to consumer goods to software products. Working in the creative industries, these men and women earn a living, feed their families, send their children to school, and support elderly parents. Counterfeiting and content theft put their jobs and their livelihoods at risk.

We have been encouraged by the work we have seen thus far to support content protection and the jobs that depend on it. Intellectual Property Enforcement Coordinator (IPEC) Victoria Espinel's attention and commitment to the work of IP protection on behalf of America's workers and businesses has been exemplary. Robust enforcement by the Departments of Justice and Homeland Security complements our own industry-wide efforts to protect theft of our content, which jeopardizes American jobs, creativity and innovation. We appreciate this opportunity to share our thoughts on these matters.



#### **Intellectual Property Enforcement Coordinator**

Ms. Espinel's efforts have been nothing less than stellar. Since her confirmation, and particularly over the last year, we have seen tremendous progress on variety of fronts, from her work with the Departments of Justice and Homeland Security to voluntary efforts with pay processors and ad networks. We look forward to hearing more about these and other efforts under consideration by the IPEC.

#### **Department of Homeland Security**

We commend the efforts of the Immigration and Customs Enforcement (ICE) agency to take the lead in combating online digital theft. ICE and the ICE-led National Intellectual Property Right Coordination Center (IPR Center) increased investigations in FY10 by 42 percent over FY09, and are on track for a 45 percent increase in FY11 over FY10. It is important to note that the leadership of the IPR Center has taken on this initiative even though the center receives no direct appropriation and has not yet been authorized. We encourage the Committee, through its oversight, to ensure the IPR Center remains a strong and reliable partner in federal intellectual property rights enforcement for years to come.

While online digital theft is a major focus of our content protection efforts, we cannot overstate the importance of the Customs and Border Patrol (CBP), whose men and women serve as the first line of defense against importation of counterfeit hard goods and circumvention devices into this country. We commend the Committee for including an amendment to the Trade Secrets Act in S. 968, the PROTECT IP Act, to enable CBP to work more closely with rights holders to identify counterfeit goods.

#### **Department of Justice**

We look forward to the testimony of the Criminal Division and the Federal Bureau of Investigation (FBI). Pursuant to the Chairman's PRO-IP Act, Congress appropriated funding in FY09 and FY10 for dedicated intellectual property agent positions for the FBI, as well as funding for dedicated federal prosecutors in FY10. Now that all these agents and prosecutors have been deployed, we look forward to seeing more robust intellectual property enforcement by the FBI.

The President's FY12 budget includes a request for \$2.95 million and six attorney positions, designated "International Computer Hacking and Intellectual Property Coordinators (ICHIPs)," to serve as Department of Justice Attachés overseas to fight transnational crime with an emphasis on intellectual property. The demise of the State Department-funded Intellectual Property Law Enforcement Coordinators (IPLC) in Sofia, Bulgaria and Bangkok, Thailand was a grave concern for our industry. We are hopeful that the Congress will strongly consider the President's request to fund these positions.

Again, our thanks for holding this important hearing on behalf of the 2.4 million people working in the film entertainment industry.

Sincerely,

The Motion Picture Association of America, Inc. (MPAA)

Paramount Pictures Corporation  
Sony Pictures Entertainment Inc.  
Twentieth Century Fox Film Corporation  
Universal City Studios LLC  
Walt Disney Studios Motion Pictures  
Warner Bros. Entertainment Inc.

RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC., (RIAA), MITCH BAINWOL,  
CHAIRMAN AND CEO, WASHINGTON, DC, JUNE 21, 2011, LETTER



June 21, 2011

Dear Chairman Leahy:

On behalf of the RIAA<sup>1</sup> and its member companies, I am writing to recognize the important anti-piracy work of the U.S. Immigration and Customs Enforcement Department. ICE's significant 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 ongoing program, Operation In Our Sites. This continuing effort 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 online, and for taking the necessary steps to ensure they are properly protected. We look forward to working with the Department and other interested parties in the future.

Sincerely,

Mitch Bainwol  
Chairman and CEO

cc: Senate Judiciary Committee

<sup>1</sup> 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.

U.S. CHAMBER OF COMMERCE, WASHINGTON, DC, STATEMENT



---

## **Statement** of the U.S. Chamber of Commerce

---

**ON:** Hearing: "Oversight of Intellectual Property Law  
Enforcement Efforts"

**TO:** Senate Committee on the Judiciary

**DATE:** June 21, 2011

---

The Chamber's mission is to advance human progress through an economic,  
political and social system based on individual freedom,  
incentive, initiative, opportunity and responsibility.

The U.S. Chamber of Commerce is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

More than 96 percent of the Chamber's members are small businesses with 100 or fewer employees, 70 percent of which have 10 or fewer employees. Yet, virtually all of the nation's largest companies are also active members. We are particularly cognizant of the problems of smaller businesses, as well as issues facing the business community at large.

Besides representing a cross-section of the American business community in terms of number of employees, the Chamber represents a wide management spectrum by type of business and location. Each major classification of American business -- manufacturing, retailing, services, construction, wholesaling, and finance -- is represented. Also, the Chamber has substantial membership in all 50 states.

The Chamber's international reach is substantial as well. It believes that global interdependence provides an opportunity, not a threat. In addition to the U.S. Chamber of Commerce's 115 American Chambers of Commerce abroad, an increasing number of members are engaged in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on national issues are developed by a cross-section of Chamber members serving on committees, subcommittees, and task forces. More than 1,000 business people participate in this process.

**Statement submitted by the U.S. Chamber of Commerce  
Senate Committee on the Judiciary  
Hearing on: "Oversight of Intellectual Property Law Enforcement Efforts"  
Wednesday, June 22, 2011**

---

The U.S. Chamber of Commerce's Global Intellectual Property Center (GIPC) commends the Senate Committee on the Judiciary for holding this important hearing, and we thank the Senate Judiciary Committee for working on a bipartisan basis to support intellectual property (IP) issues at home and abroad. The GIPC, representing a broad spectrum of IP-intensive companies, is dedicated to protecting and promoting the creativity and innovation that serve as key engines of job creation, economic growth, and global development in the 21st Century.

IP-based industries account for more than \$7.7 trillion of the U.S. gross domestic output, drive 60 percent of U.S. exports, and employ more than 19 million Americans. The global IP system is designed to spur creativity and innovation, and promote the spread of knowledge by protecting creators' and inventors' rights. This time-proven system also helps provide assurance to consumers that the products they use are authentic, safe, and effective. Further, sound IP policies and the enforcement of IP rights in the United States and abroad are essential to advancing U.S. and global economic recovery, driving America's competitiveness and export growth, and creating high-quality, high-paying American jobs.

America's innovative economy faces growing threats from counterfeiting and piracy networks that operate both online and in the traditional marketplace. In addition, some foreign governments and their allies are seeking to weaken IP rights and undermine patent, trademark, and copyright protections around the world. Today, America's business sectors invest heavily in measures to prevent and investigate IP theft. But, the private sector can only do so much. Congress and the Administration must also be committed to implementing sound IP policies and sustaining strong IP enforcement efforts in the United States and abroad. The GIPC appreciates Congress and the Obama Administration's efforts to protect U.S. intellectual property and looks forward to continuing to work to foster job creation and economic recovery in our most innovative and creative industries by addressing some of the biggest challenges to effective IP protection. The GIPC would like to point to some notable accomplishments of the Administration's on-going efforts to protect IP.

The Intellectual Property Enforcement Coordinator (IPEC) is central to the enforcement efforts of the Administration, and the GIPC believes that since her Senate confirmation in late 2009, Ms. Victoria Espinel has demonstrated a strong commitment to advancing measures that will result in more effective enforcement of IP rights. When she testified before Congress in March, Ms. Espinel proposed 20 legislative recommendations aimed at improving IP enforcement. The IPEC's office also brought forth a strategy to fight counterfeit drugs, an issue championed by Vice President Biden, to rid these deadly products from the online marketplace. Ms. Espinel has crafted a proactive and comprehensive strategy to fight against criminal networks and others who seek to steal Americans' IP. The IPEC's office has made tremendous progress despite having limited resources, staff, and budget. We're hopeful the accomplishments outlined in Ms. Espinel's testimony will prove to the Committee that these programs are working and will succeed in the future only with the requisite resources.

Immigration and Customs Enforcement (ICE) under the leadership of Director John Morton and Assistant Deputy Director Erik Barnett, have increased efforts to stop online IP theft through its “Operation In Our Sites” initiative. Operation In Our Sites has led to the seizure of more than 130 rogue websites—websites used to sell or provide access to counterfeit and pirated products. While some of these sites have reappeared, interestingly, many more, after seeing that U.S. law enforcement is serious about combating this threat, have left the marketplace before ICE and the Department of Justice have had the opportunity to shut them down. The GIPC applauds the ongoing work of ICE and extends full support on behalf of the business community in recognition of their efforts.

The Administration has made tremendous progress in fighting IP theft; however, if America is to continue to lead the world in innovation and creativity, it is imperative that the Administration and Congress continue to make intellectual property protection a top priority. The GIPC remains committed to working with Congress and the Administration to accomplish the following priorities during the coming year:

**Combat Rogue Websites**—New online technologies and high-speed Internet access greatly benefit the global economy and enable consumer access to a growing range of goods and services. However, rogue websites garner 53 billion visits a year. These websites offer illegal copies and streams of copyrighted content, and sell dangerously defective products which not only pose a risk to consumer health and safety, but severely undermine sectors of our economy that have historically provided secure, high-paying jobs. In May, the Chairman Leahy, along with Ranking Member Grassley, Senator Hatch, and a bi-partisan group of co-sponsors introduced S. 968, the PROTECT IP Act, which the Committee subsequently reported by voice vote. The GIPC strongly supports this measure aimed at cutting foreign rogue websites off from the U.S. marketplace and looks forward to working with congressional leadership to support the enactment of legislation that will effectively deal with this growing problem. We also look forward to working with the Administration to secure its support for this much needed legislation.

**Provide Deterrent Penalties for Online Theft**—The theft of content online is incredibly lucrative. Accordingly, the penalties must be high in order to deter this activity. Currently, it can be a crime to infringe copyright through the unauthorized streaming of copyrighted works. But the penalty may only be for a misdemeanor. Congress should clarify, as S. 978 would, that streaming that already meets the definition of criminal copyright infringement can be punishable as a felony. We agree with the sponsors of the bill, who have indicated it is their intent that the legislation focus on criminal activity and that it should not subject legitimate business disputes to felony prosecutions.

**Support the Advancement of Trade Agreements with Modern Day IP Provisions**—With more than 95 percent of the world’s customers living outside of the United States, it is essential that Congress advance the conclusion and implementation of trade agreements with strong IP provisions that protect America’s creations and innovations. The GIPC urges Congress to approve swiftly the pending trade agreements with Korea, Colombia and Panama. In 2011, Congress and the Administration must make it a top priority to support inclusion of the highest

IP standards in the Trans-Pacific Partnership Agreement (TPP). It is essential to America's continued competitiveness and export growth that the U.S. ensures the TPP includes modern IP provisions that are at least as ambitious as those contained in the recently finalized U.S.-Korea Free Trade Agreement (KORUS) agreement.

**Expand Government Resources Dedicated to Enforce IP rights, Starting with the IPEC—**The GIPC urges Congress to expand the dedicated resources for IP enforcement activities while crafting appropriations legislation for FY12. Congress should ensure that the IPEC has the requisite resources and dedicated staff to successfully carry out her duties as outlined in the PRO-IP Act and the National IP Strategy. The GIPC also urges Congress to enact legislation that expands the current IP attaché program into additional countries to enhance IP assistance to U.S. businesses operating abroad.

**Work with Congress on Legislation to Strengthen IP Protection and Enforcement—**The GIPC believes the Administration should work with Congress to enact legislation that enables the federal government to better protect Americans' IP rights domestically and abroad. In the 111th Congress, S. 1631, the "Customs Facilitation and Trade Enforcement Reauthorization Act of 2009," was introduced with important provisions to improve the capability of U.S. Customs and Border Protection (CBP) and Immigration Customs Enforcement (ICE) to prevent counterfeit goods from entering the United States. The GIPC strongly supports this legislation and looks forward to continuing to work with the Administration, Congress and interested stakeholders to enact a similar bill into law in 2011.

The GIPC is also eager to work with Congress to enact legislation to improve the U.S. Trade Representative's "Special 301" process by enhancing the tools available to the Administration to engage more effectively with nations that fail to respect or enforce the rights of America's innovators and/or live up to their international IP obligations. This legislation should require an action plan for Priority Watch List countries that includes clear benchmarks to measure performance, and meaningful consequences for nations that fail to perform.

#### **Conclusion**

The Obama administration can point to a series of accomplishments in support of IP enforcement. The challenges facing America and the world today make Congress' continued support for IP rights—and the swift passage of legislation to protect and promote IP at home and abroad—essential. The GIPC believes Congress, the Administration, the business community, labor, and other stakeholders can work collaboratively to safeguard and create jobs, while protecting consumer health and safety, by protecting the rights of America's inventors, artists, and entrepreneurs. The GIPC remains eager to work with Congress to offer the business community's perspective, expertise, and assistance on these issues.