

# 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 indispensible 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. <u>High-Level Commitment to Intellectual Property Enforcement</u>

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 piecury 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.1 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 severalmonth 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 transborder 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 (IPLEC) 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)2 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.