# United States Department of Justice

---

# PRO IP Act
# First Annual Report 2008-2009


**Submitted to the United States Congress**
**October 13, 2009**

# PRO IP ACT INITIAL ANNUAL REPORT OF THE ATTORNEY GENERAL 2008-2009

## INTRODUCTION

The Department of Justice (the "Department") is pleased to submit this First Annual PRO IP Act Report to the United States Congress pursuant to section 404 of the *Prioritizing Resources and Organization for Intellectual Property Act of 2008* ("PRO IP Act" or "Act"), Pub. L. No. 110-403. The Act imposes a number of annual reporting requirements on the Attorney General, including actions the Department has taken to implement Title IV of the Act ("Department of Justice Programs") and "a summary of the efforts, activities, and resources the Department has allocated in the five years prior to the date of enactment of the Act, as well as the one-year period following such date of enactment." The Act requires similar reporting by the Director of the Federal Bureau of Investigation ("FBI") on its intellectual property ("IP") enforcement efforts pursuant to Title IV of the Act both for the five years prior to enactment of the Act and the one-year period following enactment of the Act.

Because the first annual report responds to a number of overlapping or related requests for information, the Department herein will first provide a summary of its overall IP enforcement efforts in the five years prior to enactment of the PRO IP Act in October 2008, followed by a report on actions taken since enactment.

In addition, to the extent a particular request seeks information maintained by the FBI, the Department respectfully refers Congress to the FBI's Initial Annual PRO IP Act Report.

# I. REVIEW OF THE DEPARTMENT'S IP ENFORCEMENT EFFORTS IN THE FIVE YEARS PRECEDING ENACTMENT OF THE PRO IP ACT

Section 404(b) of the Act identifies those areas that the Attorney General should include in the initial report to Congress. Those provisions and the Department's efforts to implement them are set forth below.

Section 404(b) of the PRO IP Act states in pertinent part:

*"INITIAL REPORT OF THE ATTORNEY GENERAL.—The first report required to be submitted by the Attorney General under subsection (a) shall include a summary of the efforts, activities, and resources the Department of Justice has allocated in the five years prior to the date of enactment of this Act, as well as the one-year period following such date of enactment, to the enforcement, investigation, and prosecution of intellectual property crimes, including—*

*(1) a review of the policies and efforts of the Department of Justice related to the prevention and investigation of intellectual property crimes, including efforts at the Office of Justice Programs, the Criminal Division of the Department of Justice, the Executive Office of United States Attorneys, the Office of the Attorney General, the Office of the Deputy Attorney General, the Office of Legal Policy, and any other agency or bureau of the Department of Justice whose activities relate to intellectual property;*

*(2) a summary of the overall successes and failures of such policies and efforts;*

*(3) a review of the investigative and prosecution activity of the Department of Justice with respect to intellectual property crimes, including—*
*(A) the number of investigations initiated related to such crimes;*
*(B) the number of arrests related to such crimes; and*
*(C) the number of prosecutions for such crimes, including—*
*(i) the number of defendants involved in such prosecutions;*
*(ii) whether the prosecution resulted in a conviction; and*
*(iii) the sentence and the statutory maximum for such crime, as well as the average sentence imposed for such crime; and*

*(4) a Department-wide assessment of the staff, financial resources, and other resources (such as time, technology, and training) devoted to the enforcement, investigation, and prosecution of intellectual property crimes, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting intellectual property crimes."*

## (b)(1) Review of the Department's Policies and Efforts Relating to the Prevention and Investigation of IP Crimes

The Department investigates and prosecutes a wide range of IP crimes, including those involving copyrighted works, trademarks, and trade secrets. Primary investigative and prosecutorial responsibility within the Department rests with the FBI; the U.S. Attorneys' Offices; and the Criminal Division's Computer Crime and Intellectual Property Section ("CCIPS"). In addition to enforcing existing criminal laws protecting IP, the Department has supported and contributed to most major legislative developments updating criminal IP laws, including: the PRO IP Act; the Family Entertainment and Copyright Act ("FECA"), which criminalizes "camcording" (the illegal copying of movies in a theater) and unauthorized distribution of pre-release works over the Internet; the No Electronic Theft ("NET") Act, which criminalizes the unauthorized reproduction and distribution of copyrighted works without a commercial purpose or financial gain; and the Economic Espionage Act ("EEA"), which criminalizes the theft of trade secrets.

### *CCIPS and CHIP Program*

The Department carries out its IP prosecution mission through its U.S. Attorneys' Offices and CCIPS, including a network of approximately 230 specially-trained Assistant U.S. Attorneys 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 IP laws. Fourteen CCIPS attorneys are assigned exclusively to prosecuting IP crimes and implementing the Department's IP enforcement program. These attorneys prosecute cases, assist prosecutors and investigative agents in the field, and help develop and implement the Department's overall IP enforcement strategy and legislative priorities. CCIPS attorneys are available to provide advice and guidance to agents and Assistant United States Attorneys ("AUSAs") on a 24/7 basis. CCIPS attorneys also provide training on the criminal enforcement of IP laws to prosecutors and investigative agents both domestically and abroad.

CCIPS places a high priority on fostering international cooperation and coordination in its IP enforcement efforts. CCIPS has developed relationships with foreign law enforcement through international casework as well as through training and outreach. In the past five years, CCIPS attorneys and the DOJ IP Law Enforcement Coordinators in Eastern Europe and Asia met with well over 10,000 prosecutors, judges, investigators and IP officials from over 100 countries.

The CHIP Program is a network of experienced and specially-trained federal prosecutors who aggressively pursue computer crime and IP offenses. Each of the 93 U.S. Attorneys' 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, making up a total network of over 230 specially trained prosecutors nationwide. Notably,

in the past five years, the number of CHIP Units has nearly doubled, from 13 to 25. Currently, CHIP units are located in the following 25 districts:[1]

- Alexandria, Virginia
- Atlanta, Georgia
- Boston, Massachusetts
- Chicago, Illinois
- Dallas, Texas
- Kansas City, Missouri
- Los Angeles, California
- Miami, Florida
- New York, New York (Manhattan)
- New York, New York (Brooklyn)
- Sacramento, California
- San Diego, California
- San Jose, California
- Seattle, Washington
- Nashville, Tennessee
- Orlando, Florida
- Pittsburgh, Pennsylvania
- Washington, D.C.
- Austin, Texas
- Baltimore, Maryland
- Denver, Colorado
- Detroit, Michigan
- Newark, New Jersey
- New Haven, Connecticut
- Philadelphia, Pennsylvania

In 2006, the Deputy Attorney General issued guidance to all U.S. Attorneys' Offices setting forth the four program responsibilities of CHIP coordinators and CHIP Unit prosecutors:

(1) Prosecuting computer crime and IP offenses;
(2) Serving as the district's legal counsel on matters relating to those offenses, and 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.

[1] The Criminal Division and the Executive Office for United States Attorneys ("EOUSA") have worked closely with the FBI to ensure that the new IP-focused agents provided for in the PRO IP Act will be deployed in the districts with the CHIP Units handling the largest number of IP cases, and will continue to work with the FBI to ensure that those agents will be equipped to develop further the IP prosecution strategies that exist in those districts.

***Inter- and Intra-Agency Efforts***

In addition to aggressively investigating and prosecuting IP crimes domestically, the Department also has worked closely with other federal agencies (e.g., the Department of State, the Department of Homeland Security ("DHS")) to improve IP enforcement overseas, including: training investigators and prosecutors in the investigation and prosecution of IP crimes; contributing to the US Trade Representative's Special 301 process of evaluating the adequacy of our trading partners' criminal IP laws and enforcement regimes; helping to catalogue and review the U.S. government's IPR training programs abroad; evaluating the need for legislative changes to key federal statutes and the U.S. Sentencing Guidelines to address changing technology and increasingly sophisticated methods of committing IP offenses; drafting and supporting legislation to fill gaps or inadequacies in existing law; and implementing an aggressive international program to promote cooperative enforcement efforts with our trading partners and to improve substantive laws and enforcement regimes in other countries.

The Department has long recognized the importance of a coordinated approach to IP issues, and it has treated IP enforcement as an agency-wide priority. In March 2004 the Attorney General announced the creation of the Department of Justice's Task Force on Intellectual Property ("Task Force"). The Task Force undertook a thorough and detailed examination of the agency-wide approach to IP enforcement, including criminal enforcement, international cooperation, civil and antitrust issues, legislation, and prevention. The Task Force's work culminated in a 2004 report, which identified 31 recommendations to improve the Department's overall IP enforcement efforts. In 2006, the Department issued a comprehensive progress report that indicated it had implemented or was in the process of implementing all 31 of the Task Force's original recommendations. The initial October 2004 *Report Of The Department Of Justice's Task Force On Intellectual Property*, as well as the subsequent June 2006 *Progress Report of the Department of Justice's Task Force on Intellectual Property*, are appended hereto and may be found online at http://www.cybercrime.gov/IPTaskForceReport.pdf and http://www.cybercrime.gov/2006IPTFProgressReport(6-19-06).pdf.

As established by the Task Force, the Department's IP enforcement goals can be summarized as follows:

- The laws protecting IP rights must be enforced.

- The federal government and IP owners have a collective responsibility to take action against violations of federal IP laws.

- The Department should take a leading role in the prosecution of the most serious violations of the laws protecting copyrights, trademarks, and trade secrets, typically cases that are complex and large in scale, and threaten our economic national security or involve a threat to the public health and welfare.

- The federal government should punish those who misuse innovative technologies rather than innovation itself.

- IP enforcement must include the coordinated and cooperative efforts of foreign governments. The global nature of IP crime requires the informal assistance of foreign governments and their law enforcement agencies, active enforcement of their own IP laws, and formal international cooperation through treaties and international agreements.

To carry out those principles, in its 2004 report, the Task Force identified a set of 12 policy and practice recommendations to increase criminal enforcement of IP laws. In the five years preceding enactment of the PRO IP Act, the Department implemented, or continued to implement, each of those 12 recommendations:

(1) The creation of additional CHIP Units in regions of the country where IP producers significantly contribute to the national economy;

(2) The reinforcement and expansion of existing CHIP Units located in key regions where IP offenses have increased, and where the CHIP Units have effectively developed programs to prosecute CHIP-related cases, coordinate law enforcement activity, and promote public awareness programs;

(3) The designation of CHIP Coordinators in every federal prosecutor's office, who will be responsible for IP enforcement in that region;

(4) Examination of the need to increase resources for the CCIPS to address additional IP concerns;

(5) Recommending that the FBI increase the number of Special Agents assigned to IP investigations, as the Justice Department itself increases the number of prosecutors assigned to IP enforcement concerns;

(6) Recommending that the FBI increase the number of personnel assigned to search for digital evidence in IP cases;

(7) Prosecuting more nationwide and international criminal organizations that commit IP crimes;

(8) Enhancing programs to train prosecutors and law enforcement agents investigating IP offenses;

(9) Aggressively prosecuting IP offenses that endanger the public's health or safety;

(10) Emphasizing the importance of charging IP offenses in every type of investigation where such charges are applicable, including organized crime, fraud, and illegal international smuggling;

(11) Enhancing education and encouragement of victims of IP offenses and industry representatives to cooperate in criminal investigations, including:

(A) Encouraging victims to report IP crime to law enforcement agencies;
(B) Distributing the "Department of Justice Guide to Reporting Intellectual Property Crime" to victims and industry representatives regarding federal IP offenses; and
(C) Hosting a conference with victims and industry representatives to educate participants on how they can assist in law enforcement investigations; and

(12) Issuing internal guidance to federal prosecutors regarding how victims can assist prosecutors in IP cases.

## (b)(2) Summary of the Overall Successes and Failures of Such Policies and Efforts

As a result of successfully applying and updating the 12 policies and recommendations set forth in the 2004 Task Force Report over the course of the past five years, the Department has achieved notable success both domestically and abroad. The Department's achievements and progress were reported to Congress in each of the five years preceding enactment of the PRO IP Act in the annual report to Congress of the National Intellectual Property Law Enforcement Coordination Council, which the Department co-chaired.

Although the Task Force concluded its work in 2008, the Department has continued to implement its recommendations and continues to pursue criminal enforcement of IP rights vigorously. Some of the Department's more recent efforts are highlighted below:

### *Prosecution Initiatives*

#### Health and Safety

The Department's health and safety initiative brings together private, state, and federal enforcement resources and is designed to address the proliferation of counterfeit goods posing a danger to consumers, including counterfeit and illegally prescribed

pharmaceuticals. To date, this initiative has resulted in a number of significant prosecutions, including those set forth below.[2]

- *Defendant sentenced to 48 months' imprisonment for trafficking in more than $400,000 worth of counterfeit pharmaceuticals.* On July 17, 2008, Iyad Dogmosh, a Jordanian national, was sentenced in the District of Maryland to 48 months in prison for trafficking in more than 38,000 counterfeit Viagra tablets. Testing revealed that some tablets contained a chemical, which if consumed with alcoholic beverages, could cause symptoms including abdominal cramps, nausea, vomiting, and headaches. The wholesale cost for the legitimate pills would have been approximately $400,000 at the time of the defendant's crimes.

- *International distributor of counterfeit pharmaceuticals sentenced after extradition from Thailand.* On November 21, 2008, Randy Gonzales, a citizen of the Republic of the Philippines, was sentenced to 20 months in prison in the Southern District of Texas for participating in a conspiracy to import and distribute counterfeit Viagra and Cialis, which he admitted to advertising and selling over the Internet. During the year-long investigation, United States Immigration and Customs Enforcement ("ICE") agents seized more than 75,000 counterfeit Viagra and Cialis tablets, valued at more than $776,000. Gonzales was extradited to the United States from Thailand and is the first foreign national to be extradited to the United States for conspiring to import and distribute counterfeit pharmaceuticals.

- *Individuals sentenced for trafficking in more than half a million tubes of counterfeit toothpaste.* In March 2009, Habib Bah, 48, a citizen of Guinea, and Saifoulaye Diallo, 51, a U.S. citizen residing in Bronx, N.Y., were sentenced in the Eastern District of New York for trafficking in counterfeit toothpaste. Diallo was sentenced to two months' incarceration to be followed by 30 weekends in a residential facility, while Bah was sentenced to six months of home confinement. In August 2006, the defendants knowingly imported a shipment of approximately 82,944 tubes of counterfeit toothpaste from the People's Republic of China, with an estimated retail value of $116,951. Laboratory testing on samples revealed that the counterfeits lacked fluoride and some contained microorganisms and diethylene glycol, which is commonly used as a coolant in hydraulic systems and

[2] In 2008, EOUSA surveyed all United States Attorneys' Offices throughout the country concerning enforcement actions undertaken in FY2007 that involved counterfeit products posing a threat to consumer health or safety, such as counterfeit pharmaceuticals, electrical products or apparel containing toxic substances. The survey confirmed that prosecutors identified health and safety as among the most significant factors considered in exercising prosecutorial discretion to pursue IP cases. These offices reported prosecuting or investigating over 60 IP cases involving health and safety concerns in FY2007 (35 charged as IP offenses; 21 identified as IP but charged under other statutes; 6 ongoing investigations). These numbers likely understate the Department's criminal enforcement efforts because many health and safety cases are not identified as involving IP offenses, and instead are pursued under other statutes such as the Food, Drug, and Cosmetic Act.

brake fluids. Collectively, the defendants imported more than half a million tubes of counterfeit toothpaste from the People's Republic of China.

- *Internet distributor sentenced to 78 months' imprisonment for trafficking in fake cancer drugs.* On January 15, 2009, Kevin Xu, 36, was sentenced in the Southern District of Texas to 78 months in prison for conspiring with others in the People's Republic of China to traffic in counterfeit pharmaceutical drugs, and for introducing counterfeit and misbranded drugs into interstate commerce. The sentence was the maximum permitted within the applicable federal sentencing guideline range. During the course of his offenses, Xu shipped counterfeit Tamiflu, Plavix, Zyprexa, Aricept, and Casodex to undercover ICE agents. The counterfeit drugs appeared identical to legitimate pills but contained less active ingredient than the dosage listed on the labels, as well as unknown impurities. Pharmaceuticals bearing the same lot number as these counterfeit drugs penetrated the legitimate supply chain in London, England, prompting a massive recall for Zyprexa, Plavix, and Casodex.

- *Two individuals convicted of conspiring to manufacture and sell counterfeit oil pipeline couplings*. On August 12, 2009, Hayden B. Greene, 31, of Tulsa, Oklahoma, and James Robert Roy, 42, of Tomball, Texas, pleaded guilty to conspiring to manufacture and sell counterfeit pipe couplings in the Southern District of Texas. The defendants conspired with others in a scheme to manufacture and sell oilfield pipe couplings stamped with a counterfeit certification mark owned and registered by the American Petroleum Institute ("API"), without a license or other authorization to do so. The presence of a legitimate API monogram certifies that products and equipment used in the exploration and production of petroleum and natural gas meet certain API standards, specifications, and recommended practices. Couplings that do not meet the API standards are sold for limited service applications at substantially lower prices than API-certified products. The defendants profited by manufacturing many of the counterfeit couplings using cheaper, substandard materials. The defendants are scheduled to be sentenced on November 5, 2009, and each faces up to five years in prison.

**Protecting the Online Marketplace – Online Commercial Counterfeiting and Piracy Initiative**

Working with CHIP prosecutors nationwide and based on information provided by affected industries, CCIPS developed an initiative to target large-scale commercial distribution of counterfeit and pirated goods via the Internet on auction sites (e.g., eBay, Yahoo Auctions), classified ad sites (Craigslist, iOffer), and direct sales Web sites. To date, this initiative has resulted in the convictions of 38 individuals, including:

- *Texas man sentenced to 41 months' imprisonment for online sales of counterfeit software.* On February 17, 2009, Timothy Kyle Dunaway, 24, was sentenced in the Northern District of Texas to 41 months in prison for selling counterfeit

- *Oregon man sentenced to 48 months' imprisonment for selling counterfeit software on eBay worth $1 million.* On July 23, 2008, Jeremiah Joseph Mondello was sentenced in the District of Oregon to four years in prison for criminal copyright infringement, aggravated identity theft, and mail fraud for selling counterfeit computer software over the Internet with a retail value of more than $1 million. The defendant generated more than $400,000 in personal profit by stealing individuals' personal information and using the stolen identities to establish online payment systems, which he then used in selling copies of counterfeit software through auctions on eBay.

- *Six defendants sentenced for selling more than $25 million worth of counterfeit software on eBay.* On March 26, 2008, defendants Eric Neil Barber, Phillip Buchanan, Wendell Jay Davis, Craig J. Svestka, Robert Koster, and Yutaka Yamamoto were sentenced in the Eastern District of Wisconsin for selling a combined total of more than $25 million worth of counterfeit computer software on eBay, an Internet auction site. The defendants, acting separately, sold counterfeit copies of Rockwell Automation software, a specialized factory management application used for factory production lines and machinery. Most of the software sold on eBay had individual retail prices ranging from $900 to $11,000. The case was investigated by the FBI.

- *Man sentenced to 46 months' imprisonment for selling pirated teleradiological software to hospitals.* On July 28, 2009, Christopher Boyd, 63, was sentenced in the Western District of New York to 46 months in prison for copyright infringement and filing false tax returns in connection with his sale of pirated tele-radiological software to hospitals and outpatient facilities. In addition, Boyd was ordered to pay restitution totaling nearly $2 million to General Electric Healthcare, Inc. and Nexsys Electronics Incorporated, d/b/a Medweb, the companies which held the copyrights to the teleradiological software that Boyd illegally sold through his business B&L Medical. As a result of the fraud, numerous medical groups throughout the United States unwittingly purchased pirated teleradiological software from B&L Medical over the course of six to seven years.

- *Three sentenced for selling over $2 million in counterfeit sports jerseys on eBay.* On June 30, 2008, defendants Zachary Hurley, Jonathan Portwood and Stephen

**Protecting the Marketplace from Organized Online Crime**

The Department has also achieved unprecedented success in prosecuting large-scale, online piracy and counterfeiting organizations whose crimes seriously damage the marketplace for legitimate goods and services. The Department's efforts have focused not only on the top of the online distribution pyramid – the so-called "warez" groups that are responsible for the initial release of pirated software, music, video games, and movies to the Internet, often before their scheduled release date – but also on those lower in the global distribution chain, such as the most culpable file-sharers on peer-to-peer (P2P) networks.

- *60th felony conviction in worldwide software piracy crackdown Operation FastLink*: On March 6, 2009, Bryan Thomas Black, 30, of Waterloo, Ill., pleaded guilty to conspiracy to commit criminal infringement of a copyright for his involvement in a multinational software piracy organization that was targeted by investigators as part of "Operation Fastlink", an internationally coordinated 18-month investigation by the FBI. Operation Fastlink was one of the largest multi-national law enforcement actions ever taken against online software piracy. In April 2004, the FBI and foreign law enforcement conducted over 120 searches in 27 states and 12 foreign countries, including Belgium, Denmark, France, Germany, Hungary, Israel, the Netherlands, Singapore, Sweden, Spain, Great Britain, and Northern Ireland. The enforcement action targeted individuals worldwide who were identified by the investigation as leaders and high-level members of various international piracy organizations that operated on the Internet, known as "warez" groups.

- *Fifteen members of music piracy group convicted of conspiracy to commit criminal copyright infringement.* On September 19, 2008, Barry E. Gitarts, 25, of Brooklyn, New York, was sentenced to 18 months in prison for his role in operating a server used by the Internet music piracy group, Apocalypse Production Crew ("APC"). Gitarts was convicted by a jury in the Eastern District of Virginia of conspiracy to commit criminal copyright infringement. He was the first member of an Internet music piracy group to have gone to trial, but the fifteenth APC member to be convicted. APC acted as a so-called warez "release group" of pirated content to the Internet. Release groups are the original sources

- *First-ever P2P trial conviction.* On June 26, 2008, Daniel Dove was sentenced in the Western District of Virginia to 18 months in prison and was fined $20,000 for conspiracy and felony copyright infringement for his role as a high-ranking administrator of a peer-to-peer (P2P) Internet piracy group known as Elite Torrents. Dove administered a Web site for the group, which attracted more than 133,000 members and facilitated the illegal distribution of more than 17,800 titles – including movies, software, music and games – that were downloaded over two million times. Dove's conviction was the eighth resulting from Operation D-Elite, a federal crackdown against the illegal distribution of copyrighted works over BitTorrent P2P networks.

**Motion Picture Camcording**

The mass illegal distribution of newly-released copyrighted motion pictures – whether through online distribution of digital copies or through the sale of counterfeit DVDs – frequently starts with "camcording," the illegal recording of movies in theaters. The Motion Picture Association of America ("MPAA") has long identified camcording as the movie industry's top enforcement priority. The Department has prosecuted such infringers under the Family Entertainment Copyright Act of 2005.

- *Defendant sentenced to 21 months' imprisonment for camcording.* On October 28, 2008, Michael Dwayne Logan was sentenced in the District of Columbia to 21 months in prison for the unauthorized recording of motion pictures in a motion picture exhibition facility. Logan videotaped a major motion picture in its theatrical release, and was caught in the process of videotaping another in a Washington, D.C. movie theater. Forensic analysis of his high-definition camera, seized by agents, revealed evidence linking him to the taping of numerous other pirated copies of first-run motion pictures that were being illegally distributed.

**Protecting American Business from Commercial and State-Sponsored Trade Secret Theft**

Department prosecutors and the FBI have significantly increased their emphasis on the investigation and prosecution of commercial trade secret theft and state-sponsored economic espionage. Recent cases include:

- *Former Boeing engineer convicted of providing space shuttle trade secrets to the People's Republic of China.* On July 11, 2009, a federal judge in the Central District of California convicted former Rockwell and Boeing engineer Dongfan "Greg" Chung on one count of conspiracy to commit economic espionage and six substantive counts of economic espionage to benefit a foreign country, one count of acting as an agent of the People's Republic of China, and one count of making

- *Former Hewlett-Packard Vice President sentenced for stealing IBM trade secrets.* On December 18, 2008, Atul Malhotra, 42, was sentenced in the Northern District of California to five months in prison and a $3,000 fine for stealing trade secrets from his former employer, International Business Machines Corporation ("IBM"), where he had been employed for nearly 10 years before going to work for Hewlett Packard ("HP") as Vice President of Imaging and Printing Services. While employed at IBM, Malhotra requested confidential IBM business information that included proprietary cost data. Although the IBM Global Services pricing coordinator who provided the information specifically directed Malhotra not to distribute it due to its sensitive nature, after the defendant had gone to work for HP a few months later, he emailed the confidential IBM materials to two HP senior vice presidents with the subject line, "For Your Eyes Only."

- *First Economic Espionage Act sentencing.* Xiaodong Sheldon Meng, a software engineer, was sentenced on June 18, 2008, in the Northern District of California, to 24 months in prison for violating the Economic Espionage Act and the Arms Export Control Act (including the International Traffic in Arms Regulations). Meng previously pleaded guilty to two national security violations: one count of violating the Economic Espionage Act and one count of violating the Arms Export Control Act and the International Traffic in Arms Regulations. He committed economic espionage by misappropriating a trade secret from his former employer, Quantum3D Inc., with the intent to benefit the People's Republic of China Navy Research Center in Beijing. The misappropriated trade secret included software and source code from a visual simulation software program designed for training military fighter and commercial pilots. Meng is the first individual to be convicted for illegally exporting military source code in the United States, and the first to be sentenced under the Economic Espionage Act for foreign economic espionage.

***Outreach to the Public Sector***

The Department continues to reach out to the victims of IP crimes in a wide variety of ways, including during the operational stages of cases and through more formal training programs and conferences. For example, the Criminal Division hosted CCIPS' Third Annual IPR Industry/Law Enforcement meeting on June 11, 2009, in Washington, D.C. The meeting provided members of numerous IP industries with an opportunity to communicate directly with the law enforcement agents and prosecutors most responsible for federal criminal enforcement of IP law at the national level. The meeting was attended by high-level officials from the Department, including opening remarks by the Assistant Attorney General for the Criminal Division, and senior officials from the FBI, ICE, the United States Customs and Border Protection ("CBP"), the United States Food

and Drug Administration ("FDA") and others. More than 90 individuals attended the meeting, including representatives from over 40 trade associations and companies engaged in the pharmaceutical, software, luxury goods, electronic, apparel, motion picture, recording, soft drink, certification mark, personal hygiene, and automobile industries.

In the past three years, the Criminal Division has also organized and hosted a total of seven training seminars for victims of IP crimes in various locations around the country, including Los Angeles, CA; New York, NY; Miami, FL; San Jose, CA; Columbus, OH; and Houston, TX. These one-day instructional seminars provided businesses, private investigators, and corporate counsel an opportunity to discuss aspects of IP crime and enforcement with top federal and state prosecutors and law enforcement in their region. They also provided federal prosecutors and agents an opportunity to explain to industry how best to refer cases for investigation, as well as some of the ethical limitations placed on prosecutors when evaluating what level and type of assistance is properly accepted from victims in ongoing prosecutions. The seventh and most recent conference took place on June 24, 2009, in Seattle, Washington. The conference attracted over 100 IP rights holders, attorneys, investigators, and law enforcement officials. High-level government participation included remarks by the U.S. Attorneys for both the Western and Eastern Districts of Washington, the Attorney General for the State of Washington, two federal judges, federal prosecutors (including CCIPS and CHIP prosecutors from both districts in Washington), federal and local law enforcement (including FBI, ICE and CBP, FDA and the Seattle Police Department), and the U.S. Patent and Trademark Office ("USPTO"). The eighth regional conference is scheduled to be held in November 2009 in New York, NY, with participation by the U.S. Attorney's Offices for the Southern and Eastern Districts of New York and the District of New Jersey.

***International Outreach and Training***

The Department has also worked closely with the State Department and other federal agencies to provide training to law enforcement groups in countries and regions most affected by IP crimes. Through the IP Law Enforcement Coordinator ("IPLEC") program in Asia and Eastern Europe, direct engagement with law enforcement officials in China, and long-term projects in countries such as Mexico, South Africa, Brazil and Ukraine, the Department continues to aggressively combat IP crime outside the United States.

IP theft is a global problem, and a significant amount of pirated and counterfeit goods are produced overseas and trafficked to the United States. For that reason, the Department has significantly increased its efforts to build strong relationships with our law enforcement partners in other countries and to provide critical training programs that improve their enforcement regimes. For example, the Criminal Division has deployed experienced federal prosecutors to Bangkok, Thailand, and Sophia, Bulgaria, to serve as IPLECs for Asia and Eastern Europe. The Department also spearheaded the creation of the IP Crimes Enforcement Network ("IPCEN") for Asia, a group of 14 Asian countries

working together to disrupt the international trade in counterfeit and pirated goods. The group first met in October 2007, and met again in March 2009.[3]

Over the last five years, attorneys from CCIPS and the IPLECs in Asia and Eastern Europe have provided training and technical assistance, in addition to explaining U.S. criminal enforcement of IP laws to more than 10,000 prosecutors, investigators, judges and representatives of affected industries from over 100 countries, averaging about 3,000 a year. The Department expects to reach audiences of a similar scope in 2009.

In addition to the IPCEN and the regional IPLEC programs, the Criminal Division has identified priority countries for more intensive training and coordination efforts. Using grants from the State Department's Bureau of International Narcotics and Law Enforcement (INL), delivered through the Division's Office of Overseas Prosecutorial Development, Assistance and Training ("OPDAT"), CCIPS was able to effectively target international training efforts in several critical countries and regions in 2008.

### China

A substantial percentage of all counterfeit and pirated goods originate in China. In order to stop the flow of illicit goods into the United States, several years ago the Department prioritized developing critical and strong relationships with Chinese law enforcement. To that end, the Criminal Division and the Chinese Ministry of Public Security ("MPS") established and co-chair the IP Criminal Enforcement Working Group ("IPCEWG") of the U.S.-China Joint Liaison Group for Law Enforcement Cooperation ("JLG"). The IPCEWG has led to an open dialogue on IP enforcement, the sharing of information on selected investigations, and a number of successful joint IP operations. For example, as a result of aggressive coordination within the IPCEWG, on July 23, 2007, the FBI and MPS announced Operation Summer Solstice, the largest-ever joint criminal enforcement operation between the FBI and MPS against international organized criminal groups that manufacture and distribute counterfeit software. The Operation led to the arrest of 25 individuals in China, the dismantlement of multiple manufacturing locations, asset seizures by the Chinese government worth over $7 million, and the seizure of more than 290,000 counterfeit software CDs and certificates of authenticity in China. The seized counterfeit software had an estimated retail value of $500 million. Agents with the FBI's Los Angeles Field Office executed 24 searches and asset seizure warrants, yielding approximately $2 million in counterfeit software products, in addition to other assets seized worth over $700,000. Microsoft publicly stated that the criminal syndicate dismantled by the Operation was "believed to be the largest of its kind in the world," responsible for distributing more than $2 billion in counterfeit Microsoft software.

[3] Neither of the IPLEC positions is currently funded as an IP position through DOJ. The Eastern Europe position has been continued through a series of State Department grants, while the Asia position is filled by a DOJ Legal Attaché who is also filling the IPLEC role.

In addition to the IPCEWG meetings, DOJ arranged the first-ever bilateral IP training program with Chinese officials on online piracy. In November 2008, prosecutors and investigators from CCIPS, the United States Attorney's Office for the Eastern District of California, ICE, and the FBI engaged in a dialogue with Chinese law enforcement and IP administrative officials in Beijing, Nanjing and Shanghai on the topic of criminal enforcement of Internet IP crime. The U.S. delegation's participation was coordinated and made possible by the USPTO.

**Mexico**

Continuing its efforts of the last five years in Mexico, CCIPS organized several intensive training programs that included DHS, the Department of State, the World Customs Organization, and various branches of the Mexican government to increase cooperation in all phases of IP enforcement and in the investigation of IP crimes at the border. The programs took place in the ports of Vera Cruz, Manzanillo, and Mazatlan and used practical exercises to emphasize the importance of inter-agency cooperation between customs officials and prosecutors, Mexican criminal and administrative procedures, and criminal investigative techniques that lead to stronger IP cases and more deterrent sentences. Several representatives from affected U.S. companies and members of the U.S. Chamber of Commerce assisted as faculty.

As a result of the Criminal Division's efforts in Mexico, positive enforcement trends are developing:

- As of August 2008, Mexican authorities obtained 112 indictments, 27 convictions (more than in all of 2007), and nine sentences of incarceration. The criminal sentences for IP offenses included two four-year terms of imprisonment, and one six-year and six-month prison term, the latter being the longest prison sentence ever imposed in Mexico and in the region for copyright infringement.

- An unprecedented increase in IP-related seizures and referrals for criminal investigation by port officials who were involved in the above IP programs, including officials from the most technologically advanced ports of Mexico, Vera Cruz, and the Port of Lazaro-Cardenas. The Port of Lazaro-Cardenas is the second largest on the Pacific Coast, and it had never detained a shipment of infringing goods before the CCIPS-led training.

- Improvement in coordination between the PGR (Mexico's Office of the Attorney General), Aduanas (Mexican Customs), IMPI (Mexican Patent and Trademark Office, also in charge of civil IP enforcement), and the private sector. Mexico City police intelligence efforts have led to the investigation of five of the most important distributors of infringing goods in the capital. The Director of the Port of Manzanillo promised to use his best efforts to increase the number of IP seizures and referrals from Mexican Customs in his port to PGR.

- Seizure of eight containers from Asia containing 8.7 million blank optical disks in Manzanillo as a result of cooperation among participants from Aduanas, industry, and PGR who attended the Mazatlan training. PGR is still investigating the case, and Mexican Customs is seeking to impose large fines.

**South Africa**

Building on prior programs that provided training on investigating IP crimes in Botswana and South Africa, the Department and the U.S. State Department organized a training program in computer forensics for IP crimes in July 2008 in South Africa. Over 80 South African investigators and prosecutors participated. The program provided South African law enforcement officials with the skills they need to use electronic evidence in criminal IP investigations and other white collar crimes. A CCIPS trial attorney and a forensics technician from the CCIPS Cybercrime Lab demonstrated how to seize computers, secure and analyze electronic evidence, conduct off- and online investigations using computers, and present this evidence in court while also educating judges. To increase in-country capacity, this course also prepared South African trainers to train additional audiences. In addition, 14 instructors from the lead agencies in IP enforcement (South African Revenue Service which houses Customs, SA Police Service, and SA Department of Trade and Industry) received advance training that enabled them to participate in teaching the course to 80 participants in Johannesburg and Durban.

To increase the level of expertise of the South African judiciary in IP cases, the Department and the U.S. State Department invited more than 210 South African regional magistrates to attend the first South African Exclusive Judicial Workshop on the Proper Adjudication of Intellectual Property Cases near Johannesburg, South Africa, from November 13-15, 2008. South Africa has commercial crime courts that hear IP cases, but the sitting regional magistrates reported being unfamiliar with the technicalities of IP law. This has led to enforcement problems and a lack of adequate sentencing in criminal IP cases. This interactive workshop was developed to address these issues, to encourage an exchange between U.S. and South African experts, and to enhance law enforcement cooperation. U.S. District Judge Bernice Donald from the Western District of Tennessee and Chief Judge Edward Damich from the Court of Federal Claims provided vital contributions to the success of the workshop.

**India**

India is another country with a rapidly expanding information economy and many ties to U.S. corporations through manufacturing agreements, joint ventures, and production facilities. India is experiencing substantial domestic growth as a producer of IP in the entertainment, medical, and software fields. To help ensure that systems to protect IP keep pace with economic and business trends, the Department has worked closely with representatives of the judiciary and the private sector in India, as well as police, prosecutors, and other government officials, to help address the substantial delays and inefficiencies in the Indian court system that impose significant obstacles to effective enforcement of IP rights in India. During the past three years, the Department has

supported efforts by the Indian government, and in particular the courts in Delhi and Bangalore, to help build the necessary infrastructure for protecting IP by improving procedures for handling both civil and criminal cases. One aspect of this effort has been the Department's support for the creation of mediation centers in Delhi and Bangalore (two major business centers with rapidly-developing technology and IP-based business communities), including the provision of intensive mediation training sessions by U.S. federal judges and other experts. By allowing appropriate cases to be resolved with minimal judicial intervention, these mediation programs relieve some of the strain from the overburdened court system, afford more rapid resolution of IP disputes that can be readily settled, and provide more realistic time frames for judicial resolution of IP cases. As of November 2008, the Bangalore Mediation Center has settled nearly 3,000 disputes.

In addition to mediation center efforts, the Department's Criminal Division has also worked to improve criminal enforcement of IP violations through more efficient adjudication of criminal cases in Indian courts. In the wake of 2006 legislation permitting "plea bargaining" in India, CCIPS helped arrange training on how to use plea bargaining to resolve cases efficiently. These programs, held in India and the U.S., demonstrated how resolution of criminal cases through guilty pleas can lead to more efficient administration of justice while protecting the rights and interests of criminal defendants, crime victims, and the public, and to offer perspectives from U.S. courts on how to effectively administer high volumes of criminal cases. CCIPS also worked with Indian court authorities to implement plans that more efficiently handle criminal cases, starting with pilot projects to provide a "fast track" court option for criminal IP violations and other appropriate offenses. These pilot projects, implemented in Delhi and Bangalore in mid-2008, are intended to help the Indian courts resolve IP criminal cases by plea or trial within six months. Although, to date, the "fast track" courts in both cities have resolved a number of IP criminal cases, both court systems are still in the process of reorganization, including transferring all criminal IP cases to designated judges. The Criminal Division will continue to work with Indian enforcement authorities and representatives of rights holders and other affected groups during the coming year to further develop the expertise necessary for effective investigation, prosecution, and resolution of criminal IP violations.

**Brazil**

Brazil is the largest economy in South America. It has suffered the effects of IP crime as both counterfeit products and pirated versions of copyrighted works directly impact its citizens and its creative industries. The Department's Criminal Division has had a long and positive relationship with the Brazilian authorities, and has worked extensively with the Brazilian government during the implementation of the National Council to Combat Piracy and Counterfeiting in 2003-2005.

More recently, the Criminal Division worked directly with our Brazilian law enforcement counterparts to address specific issues in criminal enforcement. In December 2008, CCIPS, working with the DOJ Resident Legal Advisor, held a series of training programs in Sao Paulo, Rio de Janiero and Brasilia focusing on the technical

aspects of investigating IP crime. Two members of the CCIPS Cybercrime Lab, one trial attorney and the National CHIP Coordinator, along with a U.S. District Court Judge and investigators from the FBI and ICE, provided a detailed introduction to online piracy, digital evidence, and computer forensics to more than 900 Brazilian prosecutors, investigators, and judges.

### (b)(3) Investigative and Prosecution Activity of the Department with Respect to IP Crimes

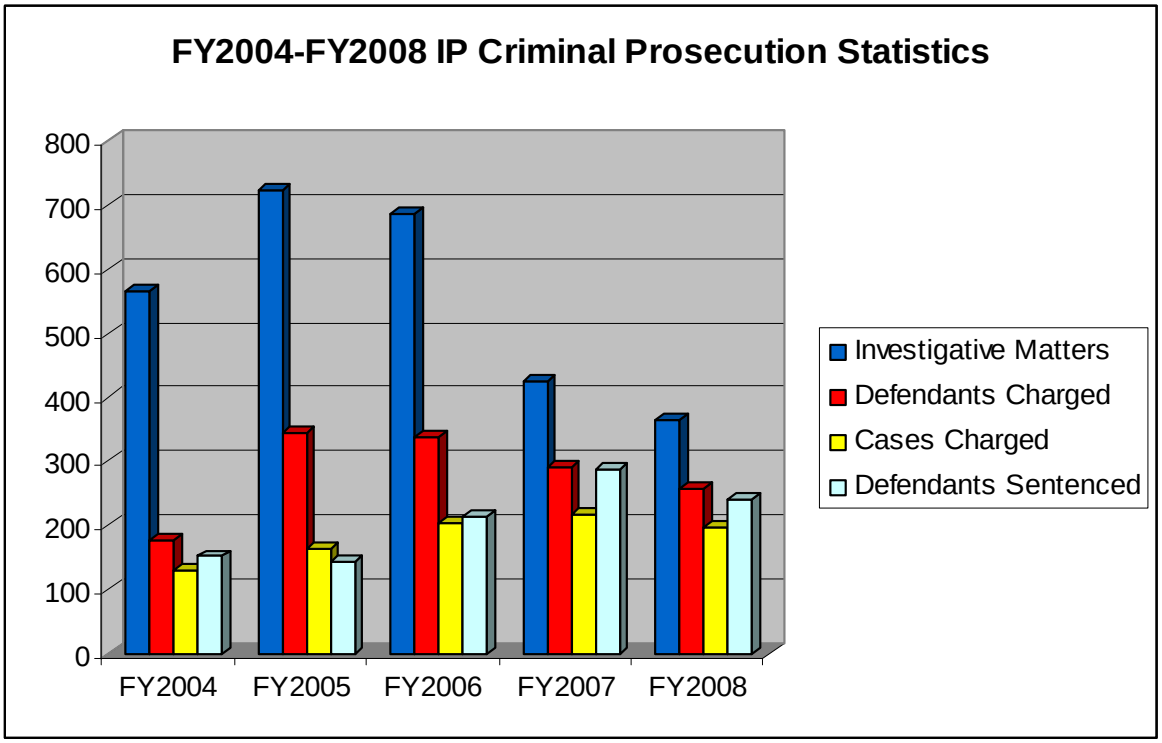
In addition to the examples of successful prosecutions listed above, there are of course hundreds of other worthy cases that could be cited. Numerical statistics do not adequately convey the quality or complexity of these prosecutions, but they are one of the metrics most frequently used to assess the effectiveness and impact of the Department's prosecution efforts.

Accordingly, we have provided the chart below that contains statistics for the five fiscal years from 2004 - 2008, listing the number of defendants and cases charged, the number of defendants sentenced, and the length of those sentences.[4] Section 404(b) of the PRO IP Act also requests statistics on the number of arrests made. Please see the Annual Report of the Federal Bureau of Investigation, provided pursuant to Section 404(c) of the PRO IP Act, for an accounting of arrest statistics.

As reflected in the chart below, the Department's unprecedented efforts to improve criminal IP enforcement have yielded, among other successes, substantial increases in federal investigations and prosecutions of IP violations. Through the dedicated efforts of U.S. Attorney's Offices, our Criminal Division, and law enforcement across the country, in FY2007, 287 defendants were convicted and sentenced on IP charges, representing a 35% increase over FY2006 (213) and a 92% increase over FY2005 (149). Additionally, the Department filed 217 IP cases in FY2007, representing a 33% increase over cases reported in FY2005. In 2008, the Department maintained generally the same level of prosecutions. To the extent there is a decrease, it parallels the decrease in the number of referrals from investigative agencies.

[4] Case statistics were compiled by the EOUSA. The chart includes data on criminal cases/defendants where the following charges were brought as any charge against a defendant: 17 U.S.C. 506 (criminal copyright infringement); 17 U.S.C. 1201 to 1205 (circumvention of copyright protection systems); 18 U.S.C. 1831 (economic espionage) & 1832 (theft of trade secret); 18 U.S.C. 2318 (counterfeit labeling): 18 U.S.C. 2319 (criminal copyright infringement); 18 U.S.C. 2319A (live musical performance infringement); 18 U.S.C. 2319B (unauthorized recording of motion pictures); 18 U.S.C. 2320 (trafficking in counterfeit goods); and 47 U.S.C. 553 or 605 (signal piracy). The statutes were grouped together in the data run in order to eliminate any double-counting of cases and/or defendants where more than one statute was charged against the same defendant. However, this chart may not include cases or defendants involving these offenses if only a conspiracy to violate one of these offenses was charged.

| District Totals | FY2004 | FY2005 | FY2006 | FY2007 | FY2008 |
|---|---|---|---|---|---|
| **Investigative Matters Received by AUSAs** | 565 | 724 | 685 | 426 | 365 |
| **Defendants Charged** | 177 | 346 | 339 | 290 | 259 |
| **Cases Charged** | 129 | 164 | 204 | 217 | 197 |
| **Defendants Sentenced** | 152 | 145 | 213 | 287 | 242 |
| **No Prison Term** | 79 | 75 | 106 | 148 | 107 |
| **1-12 Months** | 30 | 33 | 39 | 52 | 48 |
| **13-24 Months** | 18 | 18 | 28 | 37 | 45 |
| **25-36 Months** | 10 | 7 | 14 | 20 | 20 |
| **37-60 Months** | 9 | 7 | 17 | 14 | 19 |
| **60 + Months** | 6 | 5 | 9 | 16 | 3 |



### (b)(4) Department-Wide Assessment of the Resources Devoted to Enforcement of IP Crimes

The Criminal Division currently devotes 14 full-time attorneys, two paralegals and two support staff in CCIPS to IP issues. CCIPS also provides substantial support to the National Intellectual Property Rights Coordination Center ("IPR Center"), devoting two attorneys to work closely with the IPR Center to identify and de-conflict investigative leads and to pursue investigations and prosecutions. CCIPS anticipates its support to the IPR Center will increase as the Center continues to develop its operational capacity. In addition, CCIPS detailed a senior prosecutor on a full-time basis to serve as counsel to the International Organized Crime Intelligence and Operations Center in Chantilly, Virginia.

The CHIP network consists of more than 230 Assistant U.S. Attorneys who are specially trained in the investigation and prosecution of IP and computer crimes. The network includes 25 CHIP Units of between 2 to 8 CHIP prosecutors, generally located in the districts that have historically faced the highest concentration of IP and high-tech crimes.

The IPLEC program currently consists of Department attorneys in Bangkok, Thailand and Sofia, Bulgaria, who handle IP issues in Asia and Eastern Europe respectively. The IPLEC for Asia has been stationed in Bangkok since January 2006, while the IPLEC for Eastern Europe was placed in Sofia in November 2007.

The Cybercrime Lab housed in CCIPS provides support in evaluating digital evidence in IP cases, with a total of four computer forensics experts on staff. In addition to evaluating digital evidence, Cybercrime Lab technicians have provided detailed training on the use of digital forensics tools in IP cases to legal audiences around the world.

While the number of IP prosecutions and investigations generally increased between FY 2004 and FY 2007, and remained consistent in FY 2008, there has been no specially-appropriated funding to increase the number of federal prosecutors dedicated to IP criminal cases. In addition, although Congress appropriated funding in FY2009 to increase the number of FBI agents dedicated to investigate IP crimes, there was no corresponding increase in funding for prosecutors.

# REVIEW OF THE DEPARTMENT'S EFFORTS TO IMPLEMENT THE PRO IP ACT IN THE YEAR FOLLOWING ENACTMENT

Section 404(a) of the PRO IP Act requires the Attorney General to report annually to Congress on the Department's efforts to implement eight specified provisions of Title IV. Those provisions and the Department's implementation efforts are set forth below.

## (a)(1) State and Local Law Enforcement Grants

> *(1) With respect to grants issued under section 401, the number and identity of State and local law enforcement grant applicants, the number of grants issued, the dollar value of each grant, including a break down of such value showing how the recipient used the funds, the specific purpose of each grant, and the reports from recipients of the grants on the efficacy of the program supported by the grant. The Department of Justice shall use the information provided by the grant recipients to produce a statement for each individual grant. Such statement shall state whether each grantee has accomplished the purposes of the grant as established in section 401(b). Those grantees not in compliance with the requirements of this title shall be subject, but not limited to, sanctions as described in the Financial Guide issued by the Office of Justice Programs at the Department of Justice.*

Congress did not appropriate funds for the issuance of state and local law enforcement grants authorized under Section 401 of the Act.

Nevertheless, unrelated to the Act, the Office of Justice Programs ("OJP") independently offered competitive grants to support state and local IP law enforcement task forces and local IP training and technical assistance. The Intellectual Property Enforcement, Training, and Technical Assistance Program, as it is known, is designed to provide national support and improve the capacity of state and local criminal justice systems to address criminal IP enforcement, including prosecution, prevention, training, and technical assistance. Under the program, grant recipients would establish and maintain effective collaboration and coordination between state and local law enforcement, including prosecutors, multi-jurisdictional task forces, and appropriate federal agencies, specifically the FBI and U.S. Attorneys' Offices. The information shared under the program will include information about the investigation, analysis, and prosecution of matters involving IP offenses as they relate to violations of state and local criminal statutes. The program is administered by the Bureau of Justice Assistance.

The competitive grant process ended June 25, 2009, and on August 27, 2009, OJP announced that it had awarded over $2 million in grants to eight state and local law enforcement agencies and two non-profit law enforcement member organizations as follows:

- Attorney General's Office, MS ($200,000)
- Bronx County District Attorney, NY ($43,718)
- Chesterfield County, VA ($199,919)
- City of Los Angeles, CA ($199,995)
- Los Angeles County Sheriff's Department, CA ($200,000)
- New York City, NY ($200,000)
- North Carolina Department of the Secretary of State, NC ($44,485)
- Office of the Attorney General of Virginia ($17,575)

These law enforcement bodies may use the grant funds to reimburse expenses related to performing criminal enforcement operations; to educate the public to prevent, deter, and identify criminal violations of IP laws; to establish task forces exclusively to conduct investigations and forensic analyses and prosecutions; and to assist in acquiring equipment to conduct investigations and forensic analysis of evidence.

The two law enforcement member organizations that received grants were:

- National Association of Attorneys General, DC ($450,000)
- NW3C Inc. National White Collar Crime Center, VA ($450,000)

These organizations may use the grant funds to develop and provide training and technical assistance to public safety agencies in the areas of IP law enforcement. This may include the use of innovative training methodologies, such as e-training, roll call training, and academy training of both new recruits and experienced officers, prosecutors, and other justice practitioners.

**(a)(2) <u>Additional Agents of FBI</u>**

> *"(2) With respect to the additional agents of the Federal Bureau of Investigation authorized under paragraphs (1) and (2) of section 402(a), the number of investigations and actions in which such agents were engaged, the type of each action, the resolution of each action, and any penalties imposed in each action."*

Please see the Annual Report of the Federal Bureau of Investigation, which will be submitted separately pursuant to Section 404(c) of the PRO IP Act. However,

given the amount of time it necessarily takes to hire, train, and deploy new agents, it seems unlikely that there would yet be results of the type contemplated in this subsection.

**(a)(3) FBI Training**

> *"(3) With respect to the training program authorized under section 402(a)(4), the number of agents of the Federal Bureau of Investigation participating in such program, the elements of the training program, and the subject matters covered by the program."*

Please see the Annual Report of the Federal Bureau of Investigation, which will be submitted separately pursuant to Section 404(c) of the PRO IP Act.

**(a)(4) Organized Crime Plan**

> *"(4) With respect to the organized crime plan authorized under section 402(b), the number of organized crime investigations and prosecutions resulting from such plan."*

Congress has not appropriated any funds to support this provision. Nevertheless, the Department has taken a number of actions, described below, in an effort to begin implementation of this provision. Although the Department anticipates identifying investigations and prosecutions in which organized crime groups have committed IP offenses, it will be difficult to determine whether such investigations have resulted from the plan or other ongoing efforts. In addition, the Department's Organized Crime Plan, described below, will likely evolve as the Department develops intelligence relating to the links between organized crime and IP crime.

- OC Strategy:
  The Department will continue to incorporate IP into its International Organized Crime ("IOC") Strategy. As described in the Department's Overview of the Law Enforcement Strategy to Combat International Organized Crime (April 2008), "international organized crime has expanded considerably in presence, sophistication and significance – and it now threatens many aspects of how Americans live, work and do business. International organized crime promotes corruption, violence and other illegal activities, jeopardizes our border security, and causes human misery. It undermines the integrity of our banking and financial systems, commodities and securities markets, and our cyberspace. In short, international organized crime is a

national security problem that demands a strategic, targeted and concerted U.S. Government response." *See* http://www.usdoj.gov/ag/speeches/2008/ioc-strategy-public-overview.pdf. Against this backdrop, the Department established an IOC strategy that establishes an investigation and prosecution framework emphasizing the four priority areas of action:

- Marshal Information And Intelligence: Collect, synthesize, and timely disseminate the best available information and intelligence from multiple sources – including law enforcement, the intelligence community, foreign partners, and the private sector – to optimize law enforcement's ability to identify, assess, and draw connections among nationally significant IOC threats;
- Prioritize And Target The Most Significant IOC Threats: Select and target for high-impact law enforcement action the international organized crime figures and organizations that pose the greatest threat to the United States, and ensure the national coordination of investigations and prosecutions involving these targets;
- Attack From All Angles: Employ all available law enforcement and non-law enforcement tools – including drawing upon the unique expertise of every participating U.S. law enforcement agency in domestic operations, partnering with foreign counterparts to pursue cases at home and abroad, and employing U.S. government sanctions and advisories – all in a cross-cutting effort to disrupt IOC activity; and
- Enterprise Theory: Develop aggressive strategies for dismantling entire criminal organizations, especially their leadership, by using proactive investigative techniques and multi-layered prosecutions.

As Congress also recognizes, there has been an increase in reports of organized crime groups turning to trafficking in counterfeit and pirated goods as a source of illicit income, given the high profit margins and comparatively low risk involved in such crimes.

To integrate IP enforcement into the Department's overall IOC strategy, the Department will employ the following multi-pronged approach:

- IOC-2:
  CCIPS is coordinating with Organized Crime and Racketeering Section ("OCRS") to and other federal agencies through the International Organized Crime Intelligence and Operations Center ("IOC-2") to develop and implement a mechanism to address intelligence gaps as they relate to IP, among other things. The IOC-2, which was formally established on May 26, 2009, is the first multi-agency body within the United States Government to bring partner agencies together to combat international organized crime. IOC-2 collects, synthesizes, and disseminates information and intelligence from multiple sources to enable federal law enforcement to prioritize and target the individuals and organizations that pose the greatest international organized crime threat to the United States.

Understanding that international criminal organizations are profit-driven, IOC-2 also helps investigators and prosecutors to target the criminal proceeds and assets of international criminal organizations. The FBI and DHS are among the nine agencies participating in the IOC-2.

- IOC-2 Detail:
  CCIPS has detailed a senior attorney to the OCRS to act as the Counsel to the IOC-2. Among other duties, this attorney will oversee all functions of the IOC-2 Legal Division, including but not limited to providing advice and guidance on legal and policy issues, and coordinating and de-conflicting matters involving judicial process and other prosecutorial activities proscribed by statute, regulation, or policy. The Counsel is also responsible for overseeing the work of all staff assigned to the Legal Division and for coordinating, when appropriate, with Members' Agency counsel.

  In addition to his service as Counsel to IOC-2, until the permanent Chief of Intelligence was recently put in place, the CCIPS senior attorney also served as Acting Chief of Intelligence. In this capacity, he oversaw all functions carried out by the IOC-2 Intelligence Division at the OFC location, including but not limited to information fusion and analysis, and sharing of intelligence products of operational value with the field.

  Finally, as part of the Management structure of IOC-2, the CCIPS senior attorney will participate in overseeing IOC's daily operations and will report to the Attorney General's Organized Crime Council ("AGOCC").[5]

- IOC-2 IP Data Contributions:
  Working through the IOC-2 senior staff, CCIPS, OCRS, the FBI, DHS, and other relevant participating federal agencies will contribute critical IP-related intelligence and case information to the IOC-2 data pool. CCIPS is working with member agencies to ensure that IOC-2 is adequately staffed by representatives familiar with IP offenses. Once the IOC-2 is fully operational and incorporates data sources related to IP offenses, it will allow CCIPS to identify relevant organized crime cases that overlap with IP offenses.

[5] The AGOCC is comprised of 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; United States Secret Service; Internal Revenue Service, Criminal Investigation; United States Postal Inspection Service; United States Department of State, Bureau of Diplomatic Security; and the United States Department of Labor, Office of the Inspector General.

- Training:
  During the past year, the Criminal Division provided a number of training programs that included agents investigating IP crimes. Although these training courses covered a range of IP enforcement issues, each course highlighted the role of organized criminal syndicates in the global distribution of pirated and counterfeit goods. Examples of such training included:

  - In September 2009, the Criminal Division coordinated with the FBI to provide training to FBI Special Agents assigned to investigate IP crimes. The training took place in San Jose, California, and included three CCIPS instructors.

  - In September 2009, CCIPS organized and taught the Complex Online Crime Seminar at the National Advocacy Center ("NAC") in Columbia, South Carolina. This seminar was attended by both prosecutors and federal agents. Using a case scenario involving IP crime, the course provided a number of strategies and techniques for investigating criminal IP offenses.

  - In October 2008 and June 2009, CCIPS provided IP enforcement training to agents from federal law enforcement agencies stationed at the National Intellectual Property Rights Coordination Center in Arlington, Virginia. Among other topics, the training emphasized the importance of links between organized crime and IP.

  - OCRS hosted its annual Strike Force Chiefs' Conference from October 7-8, 2009. In addition to strongly emphasizing international organized crime generally, the conference also touched on the links between organized crime and IP.

  - CCIPS is revising its Intellectual Property Seminar, which will next be held at the NAC in April 2010, to incorporate teaching blocks that focus on international organized crime. This course will include both prosecutors and federal agents.

  - The Criminal Division and its law enforcement partners will continue to look for opportunities to provide training to federal agents and prosecutors that emphasizes the potential links between organized crime and IP offenses.

### (a)(5) Authorized Funds Under Section 403

(5) *With respect to the authorizations under section 403—*

*(A) the number of law enforcement officers hired and the number trained;*
*(B) the number and type of investigations and prosecutions resulting from the hiring and training of such law enforcement officers;*
*(C) the defendants involved in any such prosecutions;*
*(D) any penalties imposed in each such successful prosecution;*
*(E) the advanced tools of forensic science procured to investigate, prosecute, and study computer hacking or intellectual property crimes; and*
*(F) the number and type of investigations and prosecutions in such tools were used."*

The Department, through the Office of the Deputy Attorney General, the Criminal Division and EOUSA, worked closely with the FBI to determine which field offices to assign the newly designated IP FBI Special Agents. As of September 2009, the FBI had deployed 26 agents, who are dedicated solely to the investigation of IP crimes, to 19 field offices supporting most CHIP Units. In addition, to date the FBI has deployed a Unit Chief, two Supervisory Special Agents, and one Special Agent (with two additional agents designated but not yet deployed) to the IPR Center to work with CCIPS and to oversee a national IP program. Please see the Annual Report of the Federal Bureau of Investigation, provided separately under Section 404(c) of the PRO IP Act, for further details.

### (a)(6) Other Relevant Information

"(6) *Any other information that the Attorney General may consider relevant to inform Congress on the effective use of the resources authorized under sections 401, 402, and 403."*

The Department received appropriations only for the hiring and placement of additional FBI agents. For possible additional relevant information pertaining to those agent resources, please refer to the FBI's Annual Report provided pursuant to Section 404(c).

## (a)(7) Efforts, Activities and Resources Allocated to the Enforcement of IP Crimes

*(7) A summary of the efforts, activities, and resources the Department of Justice has allocated to the enforcement, investigation, and prosecution of intellectual property crimes, including –*

*(A) a review of the policies and efforts of the Department of Justice related to the prevention and investigation of intellectual property crimes, including efforts at the Office of Justice Programs, the Criminal Division of the Department of Justice, the Executive Office of United States Attorneys, the Office of the Attorney General, the Office of the Deputy Attorney General, the Office of Legal Policy, and any other agency or bureau of the Department of Justice whose activities relate to intellectual property;*

*(B) a summary of the overall successes and failures of such policies and efforts;*

*(C) a review of the investigative and prosecution activity of the Department of Justice with respect to intellectual property crimes, including –*

*(i) the number of investigations initiated related to such crimes;*
*(ii) the number of arrests related to such crimes; and*
*(iii) the number of prosecutions for such crimes, including—*

*(I) the number of defendants involved in such prosecutions;*
*(II) whether the prosecution resulted in a conviction; and*
*(III) the sentence and the statutory maximum for such crime, as well as the average sentence imposed for such crime; and*

*(D) a Department-wide assessment of the staff, financial resources, and other resources (such as time, technology, and training) devoted to the enforcement, investigation, and prosecution of intellectual property crimes, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting intellectual property crimes.*

The Department's response to the five-year reporting requirements in subsection 404(b), above, includes information, policies, and initiatives responsive to this request. Complete statistical data for FY 2009 is not yet available, but will be submitted with the Attorney General's Annual Report to Congress in early FY 2010.

**(a)(8) Efforts to Increase Efficiency**

> *"(8) A summary of the efforts, activities, and resources that the Department of Justice has taken to—*
>
> *(A) minimize duplicating the efforts, materials, facilities, and procedures of any other Federal agency responsible for the enforcement, investigation, or prosecution of intellectual property crimes; and*
>
> *(B) enhance the efficiency and consistency with which Federal funds and resources are expended to enforce, investigate, or prosecute intellectual property crimes, including the extent to which the Department has utilized existing personnel, materials, technologies, and facilities."*

The Department works hard to ensure the effective use of limited resources devoted to fighting IP crime. One of the most important ways to reduce duplication of effort is to ensure that law enforcement agencies are pursuing unique case leads, and that prosecutors are not following prosecution strategies that overlap with cases in other districts. To that end, CCIPS has provided extensive and ongoing support to the newly re-opened IPR Center in Arlington, Virginia. Among other things, the IPR Center is intended to serve as an investigation clearinghouse for FBI, ICE, FDA, and others. Department attorneys will continue to work with the IPR Center to identify and de-conflict investigative leads to ensure that investigations are streamlined, not duplicated, and appropriately venued.