# United States Department of Justice

# PRO IP Act
# Annual Report FY2010

**Submitted to the United States Congress**
**December 17, 2010**

# PRO IP ACT ANNUAL REPORT OF THE ATTORNEY GENERAL FY2010

## INTRODUCTION

The Department of Justice (the "Department") submits this 2010 annual report to the United States Congress pursuant to §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 to the enforcement, investigation, and prosecution of intellectual property crimes." The Act requires similar annual 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.

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

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 during the prior fiscal year ("FY"). Those provisions and the Department's efforts to implement them during FY2010 (*i.e.*, October 1, 2009 through September 30, 2010) are set forth below.

In February 2010, the Attorney General announced the creation of the Intellectual Property Task Force ("IP Task Force"). The IP Task Force, chaired by the Deputy Attorney General and comprised of senior Department officials, has brought high-level attention and coordination to the Department's overall IP enforcement efforts. The Department's efforts, activities and allocation of resources described below were achieved under the IP Task Force's direction and support.

In addition, working closely with the Office of the Intellectual Property Coordinator ("IPEC"), the Department contributed to developing a government-wide joint strategic plan. Although the Department's implementation of the relevant criminal enforcement provisions of the joint strategic plan will be contained in the IPEC's coordinated annual report, such efforts are also contained herein as part of the Department's description of its efforts, activities and allocation of resources.

## (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 breakdown 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.*

As in FY2009, Congress did not appropriate funds in FY2010 for the issuance of state and local law enforcement grants as authorized under §401 of the Act.

Nevertheless, in keeping with IP Task Force priorities, the Office of Justice Programs ("OJP") offered competitive grants to support state and local IP law enforcement task forces and local IP training and technical assistance as authorized by the Omnibus Consolidated Appropriations Act, 2010 (Pub. L. 111-117), and as informed by §401 of the PRO IP Act. The

FY2010 Intellectual Property Enforcement 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, including 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, a component of OJP.

The competitive grant process ended May 18, 2010, and on September 30, 2010, OJP announced that it had awarded approximately $4 million in grants to 14 state and local law enforcement agencies and three non-profit organizations in support of the FY2010 Intellectual Property Enforcement Program.

The following FY2010 awards to state and local jurisdictions cover expenses related to: performing criminal enforcement operations; educating the public to prevent, deter, and identify criminal violations of IP laws; establishing task forces to conduct investigations and forensic analyses and prosecutions; and acquiring equipment to conduct investigations and forensic analysis of evidence.

| Award Number | Grantee | Amount |
|---|---|---|
| 2010-BE-BX-0001 | Attorney General's Office, Mississippi | $166,365 |
| 2010-BE-BX-0002 | City of San Antonio | $200,000 |
| 2010-BE-BX-0003 | County of Sacramento | $200,000 |
| 2010-BE-BX-0004 | North Carolina Department of the Secretary of State | $199,978 |
| 2010-BE-BX-0005 | Los Angeles County Sheriff's Department | $200,000 |
| 2010-BE-BX-0006 | Chesterfield County, VA | $200,000 |
| 2010-BE-BX-0007 | Virginia Department of State Police | $149,907 |
| 2010-BE-BX-0008 | Miami Shores Village | $64,885 |
| 2010-BE-BX-0009 | County of Fresno | $49,992 |
| 2010-BE-BX-0010 | New York County District Attorney's Office | $199,800 |
| 2010-BE-BX-0011 | Bronx County District Attorney | $113,103 |
| 2010-BE-BX-0012 | New York City | $192,200 |
| 2010-MU-BX-0013 | Houston Police Department | $200,000 |

In addition, OJP awarded a $400,000 grant to the City of Los Angeles Police Department to supplement its ongoing efforts in IP enforcement in partnership with the Los Angeles County Prosecutor's Office, which has resulted in an increase in arrests, search warrants served, property recovered, and investigations initiated in the area of IP crime.

Finally, OJP awarded supplemental funding to the following entities in order to increase training and technical assistance to state, local, and tribal law enforcement agencies to enhance their capacity to respond to IP crime.

- **National Crime Prevention Council ("NCPC"), $600,000:** This supplement to NCPC's FY2009 competitive award will support ongoing efforts regarding the development and implementation of a national IP awareness campaign.

- **National Association of Attorneys General ("NAAG"), $300,000:** This supplement to NAAG's FY2009 competitive award will support ongoing efforts to expand the delivery

of joint law enforcement and prosecutor training on IP enforcement in partnership with the National White Collar Crime Center.

- **National White Collar Crime Center ("NW3C"), $563,770:** This supplement to NW3C's FY2009 competitive award will support ongoing efforts to expand the delivery of joint law enforcement and prosecutor training on IP enforcement in partnership with NAAG.

**(a)(2) Additional Agents of FBI**

> *"(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 §404(c) of the PRO IP Act.

**(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 §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."*

As in FY2009, Congress has not appropriated funds to support §402(b) of the PRO IP Act in FY2010.[1] Nevertheless, the Department has continued to take a number of actions, described below, in an effort to implement this provision. These actions taken include increased information sharing and coordination, training, and outreach. However, the Department will not be able to provide a specific number of prosecutions directly resulting from these increased efforts for several reasons. First, the Department can retrieve statistical information from its database based on the statute charged but not based on the type of defendant or group that committed the offense. Second, it is difficult to determine whether prosecutions involving organized crime groups have resulted directly from the Department's organized crime plan efforts or other ongoing efforts. Finally, the Department's efforts to develop and implement its plan are relatively recent. Because it often takes substantial time to investigate and prosecute an organized crime case, to the extent it is possible to correlate such investigations and prosecutions to the plan, it is unlikely that such prosecutions would have come to fruition as of yet.

As detailed in the Department's first Annual PRO IP Act Report, the Department has incorporated IP into the Attorney General's International Organized Crime ("IOC") Strategy. In addition to the ongoing efforts outlined in last year's report designed to integrate IP enforcement into the Department's overall IOC strategy, the Department has taken the following additional actions to address this important issue:

- The IP Task Force has identified IP crimes perpetrated by organized criminal syndicates as a top IP enforcement priority.

[1] Section 402(b) provides that "[s]ubject to the availability of appropriations to carry out this subsection, and not later than 180 days after the date of the enactment of this Act, the Attorney General, through the U.S. Attorneys' Offices, the Computer Crime and Intellectual Property section, and the Organized Crime and Racketeering section of the Department of Justice, and in consultation with the Federal Bureau of Investigation and other Federal law enforcement agencies, such as the Department of Homeland Security, shall create and implement a comprehensive, long-range plan to investigate and prosecute international organized crime syndicates engaging in or supporting crimes relating to the theft of intellectual property."

- The Attorney General's Organized Crime Council ("AGOCC")[2] also has prioritized IP enforcement, adopting as part of its 2010 Action Plan a specific goal to enhance law enforcement coordination in this important area.

Under the guidance of the IP Task Force and the AGOCC the Department has taken the following actions:

**Increased Information Sharing and Coordination**:

- The Department, through the Criminal Division, is continuing to coordinate with federal investigatory agencies to work with the International Organized Crime Intelligence and Operations Center ("IOC-2") in an ongoing effort to develop and implement a mechanism to both contribute data to IOC-2 and to address intelligence gaps as they relate to IP, among other things. Highlights of these efforts include:

  - CCIPS has detailed a senior attorney to IOC-2, who now serves as the Acting Director, reporting to the AGOCC.

  - Currently, all relevant agencies with a stake in criminal IP investigations are contributing IP data to IOC-2, including the FBI, ICE, and CBP.

  - IOC-2 is working with the National Intellectual Property Rights Coordination Center ("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. Such protocols will facilitate the working relationship between the IPR Center and the OCDETF Fusion Center ("OFC"), which owns and houses the COMPASS database used by IOC-2.

  - The Criminal Division's Organized Crime and Racketeering Section ("OCRS") and Computer Crime and Intellectual Property Section ("CCIPS") regularly conduct case reviews to determine whether further coordination is appropriate.

[2] 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; 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.

**Training and Outreach**

- In September 2010, the IP Law Enforcement Coordinator ("IPLEC") for Asia presented on the links between organized crime and IP at the Sendai meeting of Asia-Pacific Economic Cooperation ("APEC"). This is an ongoing effort.

- In July 2010, the Asset Forfeiture and Money Laundering Section ("AFMLS") incorporated a training block on the links between IP crime and organized crime at AFMLS' Money Laundering Seminar at the National Advocacy Center ("NAC") in Columbia, South Carolina.

- In June 2010, CCIPS and OCRS made a joint presentation at the IPR Center Symposium, "IP Theft and International Organized Crime and Terrorism - The Emerging Threat," on the Department's current efforts to address the links between IP crime and organized crime. Participating in the symposium were close to 80 copyright and trademark holders as well as federal, state, and local law enforcement officials and academics.

- In April 2010, CCIPS developed and led the IP Crimes Seminar at the NAC in Columbia, South Carolina. Both prosecutors and federal agents attended this course, which highlighted the fact that investigating and prosecuting IP offenses linked to organized crime groups is an enforcement priority of the Attorney General, and provided tools and investigative strategies to assist in this effort.

- In November 2009, OCRS and IOC-2 attended a three-day conference hosted by OLAF, the Anti Fraud Office of the European Union, focusing on counterfeit cigarette smuggling. Also participating were representatives from law enforcement authorities around Europe, North America, and other countries, prosecutors from Strike Forces around the U.S., and the U.S. Attorney for the Northern District of New York. The conference marked the first time that many of these organized crime prosecutors were significantly exposed to investigations targeting IP offenses.

**Preview of FY2011 Outreach and Training**

- In October 2010, the Attorney General delivered the keynote address at the Fourth Annual International Law Enforcement IP Crime Conference in Hong Kong, hosted by INTERPOL and Hong Kong Customs in partnership with Underwriters Laboratory. The Attorney General addressed the conference theme of "Working Together to Break Organized Crime." CCIPS also presented on several panels at the conference. In attendance at the three-day conference were more than 500 law enforcement agents, prosecutors and industry representatives from approximately 40 countries.

- In October 2010, CCIPS made a presentation to a conference of State Department Economic Officers from posts throughout sub-Saharan Africa to discuss IP crime and

the role of organized criminal groups in controlling illicit trade in counterfeits in Africa.

**Preview of Upcoming Training**

- In March 2011, CCIPS will include a training block at the annual Computer Hacking and Intellectual Property ("CHIP") conference on efforts to address organized crime and IP crime as well as a briefing by IOC-2 on the tools it offers to agents and prosecutors in this area. The conference will bring together nearly 200 Assistant U.S. Attorneys ("AUSAs") who specialize in prosecuting high tech crimes, including IP crime, and will provide cutting-edge training on legal issues and policy developments relating to the investigation and prosecution of IP and computer crime, as well as technological trends and investigative tools for obtaining and reviewing electronic evidence.

- OCRS will incorporate a training block on IP and organized crime at the annual Strike Force conference currently planned for January 2011.

- CCIPS and OCRS are working with the State Department's Bureau of International Narcotics and Law Enforcement ("INL") to develop a training program on illicit trade for members of APEC Forum, which will be held during the U.S. presidency of APEC in 2011.

- In the coming months, CCIPS and the Office of Overseas Prosecutorial Development Assistance and Training ("OPDAT") (using State Department money) will provide training in Zambia, South Africa, and Mexico on the connection between organized crime and the trade in counterfeit pharmaceuticals.

**(a)(5) Authorized Funds Under §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."*

In December 2009, Congress provided funding for the Department to appoint 15 new CHIP prosecutors to support CHIP Units nationwide. The Department, through the Office of the Deputy Attorney General, Executive Office of U.S. Attorneys and the Criminal Division, identified the following locations for the new positions: California, the District of Columbia, Maryland, Massachusetts, Michigan, New Jersey, New York, Pennsylvania, Texas, Virginia and Washington.

Please see the Annual Report of the Federal Bureau of Investigation, provided separately under §404(c) of the PRO IP Act, for details on the FBI allocation of resources.

**(a)(6) <u>Other Relevant Information</u>**

> "(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 in FY2010. For possible additional relevant information pertaining to those agent resources, please refer to the FBI's Annual Report provided pursuant to §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.*

### (a)(7)(A) 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 CCIPS. In addition, the IP Task Force provides high-level support and policy

guidance to the Department's overall IP enforcement efforts. Each of these components will be described briefly below.

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 of 2008; the Family Entertainment and Copyright Act of 2005 ("FECA"), which criminalized "camcording" (the illegal copying of movies in a theater) and unauthorized distribution of pre-release works over the Internet; the No Electronic Theft Act of 1997 ("NET Act"), which criminalized the unauthorized reproduction and distribution of copyrighted works without a commercial purpose or financial gain; and the Economic Espionage Act of 1996 ("EEA"), which criminalized the theft of trade secrets, including economic espionage.[3]

Most recently, the Department contributed to a number of legislative proposals and recommendations regarding criminal IP enforcement that are expected to be included in the IPEC's legislative recommendations to Congress in late December 2010.

***CCIPS and CHIP Program***

The Department carries out its overall IP criminal prosecution mission through its U.S. Attorneys' Offices and CCIPS, including a network of approximately 230 specially-trained federal prosecutors who make up the Department's 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 intellectual property enforcement. These attorneys prosecute criminal 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 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. It has developed relationships with foreign law enforcement through international casework as well as through training and outreach.

The CHIP program is a network of experienced and specially-trained federal prosecutors who aggressively pursue computer crime and IP offenses. Each of the 94 U.S. Attorneys' Offices has at least one CHIP coordinator. In addition, 25 U.S. Attorneys' Offices have CHIP

[3] For an overview of the Department's policies and efforts in the five years prior to the enactment of the PRO IP Act in October 2008, the Department's PRO IP Act First Annual Report 2008-2009 may be found online at http://www.cybercrime.gov/proipreport2009.pdf. Additionally, 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.

Units, with between two and eight CHIP attorneys.[4] CHIP attorneys have four major areas of responsibility including: (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.

***Interagency Coordination***

In addition to aggressively investigating and prosecuting IP crimes domestically, the Department also has worked closely with other federal agencies (*e.g.,* IPR Center, the Department of State, the Department of Homeland Security ("DHS"), the U.S. Patent and Trademark Office ("USPTO")) to improve IP enforcement overseas, including: training investigators and prosecutors in the investigation and prosecution of IP crimes; contributing to the U.S. 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 IP training programs abroad; 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.

***Intellectual Property Task Force***

In February 2010, the Attorney General announced the IP Task Force's formation as part of a Department-wide initiative to confront the growing number of domestic and international IP crimes. The IP Task Force, which is chaired by the Deputy Attorney General and comprised of senior Department officials from every component with a stake in IP enforcement, focuses on strengthening efforts to combat IP crimes through close coordination with state and local law enforcement partners as well as international counterparts. The Task Force also monitors and coordinates overall IP enforcement efforts at the Department, with an increased focus on the international aspects of IP enforcement, including the links between IP crime and international organized crime. Building on previous efforts in the Department to target IP crimes, the Task Force serves as an engine of policy development to address the evolving technological and legal landscape of this area of law enforcement.

In order to provide focused attention to particular issues, the Task Force established four working groups:

[4] CHIP Units are currently located in Alexandria, Virginia; Atlanta, Georgia; Boston, Massachusetts; Chicago, Illinois; Dallas, Texas; Kansas City, Missouri; Los Angeles, California; Miami, Florida; New York, New York; Brooklyn, New York, New York; Sacramento, California; San Diego, California; San Jose, California; Seattle, Washington; Nashville, Tennessee; Orlando, Florida; Pittsburgh, Pennsylvania; Philadelphia, Pennsylvania; Washington, D.C.; Austin, Texas; Baltimore, Maryland; Denver, Colorado; Detroit, Michigan; Newark, New Jersey; New Haven, Connecticut.

- **Enforcement Assessment / Priorities Working Group:** charged with ongoing responsibility to assess the Department's enforcement efforts, policies and strategies and to make recommendations where appropriate, including evaluating the need for legislative changes to key federal statutes and the U.S. Sentencing Guidelines to address gaps or inadequacies in existing law, changing technology, and increasingly sophisticated methods of committing IP offenses.

- **Outreach and Education Working Group:** spearheads public outreach and education activities on IP issues, including outreach to victim industry groups, the general public, and state and local governments.

- **Civil Enforcement / Policy Working Group:** charged with an ongoing responsibility to identify opportunities for increased civil IP enforcement and legislative action.

- **International Outreach and Coordination Working Group:** focuses on expanding international enforcement and capacity building efforts as well as improving relationships with foreign counterparts.

As part of its mission, the IP Task Force works closely with the IPEC. The IP Task Force assists the IPEC in recommending improvements to IP enforcement efforts, including:

- Helping to identify and develop legislative proposals;

- Developing an agenda for future international IP programs to ensure integration and reduce overlap with programs run by other agencies;

- Helping to develop a model for IP plans in selected Embassies around the world; and

- Coordinating activities through regular calls and meetings with the IPEC and relevant agencies.

The efforts undertaken under the IP Task Force's direction are described in more detail in §(a)(7)(B) below.

### (a)(7)(B) Summary of the Overall Successes and Failures of Such Policies and Efforts

As part of the IP Task Force initiative, the Department achieved notable success in FY2010 both domestically and abroad. Some of these efforts are highlighted below:

***Prosecution Initiatives***

Through its IP Task Force, the Department identified four enforcement priorities for IP investigations and prosecutions, including offenses that involve (1) health and safety, (2) links to

organized criminal networks, (3) large scale commercial counterfeiting and online commercial piracy, and (4) trade secret theft or economic espionage.

### (1) Health and Safety

The Department's health and safety initiative brings together private, state, and federal enforcement resources to address the proliferation of counterfeit goods posing a danger to consumers, including counterfeit and illegally prescribed pharmaceuticals. In FY2010, this initiative resulted in a number of significant prosecutions, including those set forth below:

- *Defendant sentenced to 30 months' imprisonment for selling counterfeit Cisco parts to Bureau of Prisons.* In September 2010, the owner of Syren Technology was sentenced to 30 months in prison for selling counterfeit Cisco networking products to the Bureau of Prisons. The investigation revealed that the defendant also sold counterfeit parts to other government agencies including the Marine Corps, Air Force, FBI, Federal Aviation Administration, and the Department of Energy, as well as to various defense contractors. (SDTX, ICE, CBP).

- *Internet distributor sentenced to 33 months' imprisonment for selling fake cancer drugs and pirated business software.* In August 2010, Hazim Gaber, 22, of Edmonton, Canada, was sentenced in the District of Arizona to 33 months in prison for selling fake cancer drugs online and more than 800 copies of pirated business software. Gaber sold what he claimed was the experimental cancer drug sodium dichloroacetate ("DCA") to 65 victims in the U.S., Canada, the United Kingdom, Belgium, and the Netherlands. Laboratory testing revealed that the substance sold contained no DCA. Gaber was arrested in Frankfurt, Germany, and was extradited to the U.S. in December 2009 for prosecution. (CCIPS, DAZ, FBI).

- *Husband and wife sentenced for their roles in scheme to distribute unapproved foreign prescription drugs.* In May 2010, Randy T. French, 53, and Sheila D. French, 44, both of Kingman, Arizona, were sentenced in the District of Arizona for their respective roles in conducting a scheme to distribute counterfeit prescription drugs by filling customers' orders with unapproved and misbranded imitation drugs from India. Randy French was sentenced to 18 months in prison, to be followed by three years of supervised release. Sheila French was sentenced to three years probation, to include 12 months of home confinement. From 2004 to 2006, the Frenches' illegal prescription drug business, "Prescription Buyers Group," generated revenues of more than $2,500,000. (DAZ, FDA-OCI, Lake Havasu City PD).

- *Operation Network Raider.* In May 2010, DOJ and DHS announced the results of Operation Network Raider, a domestic and international enforcement initiative targeting the illegal distribution of counterfeit network hardware manufactured in China. The initiative 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. The operation is a joint initiative by the FBI, ICE and CBP working with U.S.

Attorneys' Offices around the country, CCIPS, and the IPR Center. Through aggressive investigation and prosecution, the initiative sought 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. (FBI, ICE, CBP, CCIPS, USAOs).

- *Defendant sentenced to 51 months' imprisonment for trafficking counterfeit Cisco products.* In May 2010, Ehab Ashoor, 49, a Saudi citizen who resided in Sugarland, Texas, was sentenced in the Southern District of Texas to 51 months in prison and ordered to pay $119,400 in restitution to Cisco Systems. Ashoor purchased counterfeit Cisco Gigabit Interface Converters ("GBICs") from a Chinese online vendor with the intention of selling them to the U.S. Department of Defense for use by U.S. Marine Corps personnel operating in Iraq. The Marine Corps used the computer network for which the GBICs were intended to transmit troop movements, relay intelligence and maintain military base security. This case was part of Operation Network Raider. (SDTX, ICE).

- *California man pled guilty to the wholesale and retail sale of counterfeit goods including electrical power strips marked with the "UL" quality symbol.* In February 2010, Qi Jin Chen, 37, of Stockton, California, pled guilty to trafficking in counterfeit goods and to structuring cash transactions to avoid mandatory reporting requirements. During the investigation, law enforcement agents seized truckloads of counterfeit items that, if genuine, would have been valued at over $7 million. Items seized ranged from power strips marked with the "UL" quality symbol, to counterfeit purses purporting to be from Chanel, Dolce & Gabanna, and Fendi, or jewelry purporting to be from Tiffany and Juicy Couture. Chen is awaiting sentencing. In November 2010, Chen was sentenced to 26 months in prison, and was ordered to pay a $25,000 fine and $9,575 in restitution. (EDCA, USSS, IRS Financial Crimes Task Force, Placer County Sheriff's Office, Galt PD).

- *Two individuals pled guilty to trafficking in counterfeit integrated circuits and to conspiring to traffic in counterfeit integrated circuits.* In January 2010, Mustafa Abdul Aljaff, 30, and in November 2009, Neil Felahy, 32, both of Newport Coast, California, pled guilty to trafficking in counterfeit goods and to conspiring to traffic in counterfeit goods. Aljaff, Felahy, and others imported more than 13,000 integrated circuits bearing counterfeit trademarks, including military grade markings, into the U.S. from China and Hong Kong. Aljaff, Felahy, and others entered into contracts with the U.S. Navy and other government agencies for the sale of these counterfeit circuits. For the crime of conspiracy, Aljaff and Felahy each face up to five years in prison, and for the crime of trafficking in counterfeit goods, Aljaff and Felahy each face up to ten years in prison. (DDC, ICE, NCIS, DOT, CBP).

### (2) Protecting American Business from Commercial and State-Sponsored Trade Secret Theft

In FY2010, Department prosecutors and the FBI have continued their increased emphasis on the investigation and prosecution of commercial trade secret theft and state-sponsored

economic espionage. This continuing focus has led to the investigation and prosecution of ten trade-secret cases and two economic espionage cases. Recent cases include:

- *Former Bristol-Myers-Squibb employee indicted on theft of trade secrets charges.* In November 2010, Shalin Jhaveri, 29, of Syracuse, New York, pled guilty in the Northern District of New York for stealing trade secrets and proprietary information from his employer Bristol-Myers-Squibb. The indictment alleged that while employed at Bristol-Myers-Squibb as a Technical Operations Associate, Jhaveri stole numerous trade secrets as part of a plan to establish a pharmaceutical firm in his native India, which would compete with Bristol-Myers-Squibb in various world-wide markets. (NDNY, FBI, ICE).

- *Former chemist pleads guilty to stealing trade secrets valued at up to $20 million.* In September 2010, David Yen Lee, a former chemist for a northwest suburban paint manufacturing company pled guilty to theft of trade secrets, admitting that he stole numerous formulas and other proprietary information valued at up to $20 million from Valspar Corporation as he prepared to go to work for an overseas competitor. The defendant, who had been a technical director in Valspar's architectural coatings group since 2006, admitted using his access to Valspar's secure internal computer network to download approximately 160 secret formulas for paints and coatings in addition to taking other internal information from Valspar's offices. Lee is scheduled to be sentenced on December 8, 2010. (NDIL, FBI).

- *Chinese national charged with economic espionage involving theft of trade secrets from leading agricultural company based in Indianapolis*. In August 2010, a 17-count indictment was unsealed charging Kexue Huang, a 45 year-old Chinese national, with economic espionage intended to benefit China, as well as interstate and foreign transportation of stolen property. The indictment alleges that Huang, formerly of Carmel, Indiana, misappropriated and transported trade secrets and property to China while working as a research scientist at Dow AgroSciences LLC ("Dow"). While employed at Dow, he then directed university researchers in China to further develop the Dow trade secrets. He also allegedly applied for and obtained grant funding that was used to develop the stolen trade secrets. (CCIPS, SDIN, NSD, FBI).

- *Former DuPont research chemist sentenced to 14 months' imprisonment for stealing DuPont trade secrets*. In June 2010, Hong Meng, 43, a former DuPont research chemist, waived indictment and pled guilty to theft of trade secrets, and, in October 2010, Meng was sentenced to 14 months' imprisonment. While still employed at DuPont, Meng stole information related to a secret chemical process in the field of Organic Light Emitting Diodes ("OLED") technology, which is the next generation of display and lighting applications. Meng emailed confidential information regarding OLED technology to his Peking University ("PKU") email account and also saved it to his personal computer. Meng admitted making false statements to the FBI regarding whether he mailed chemical compound samples to a colleague with the request that the samples be forwarded to Meng's PKU office. (DDE, FBI).

- *Former Boeing engineer sentenced to 188 months' imprisonment for providing space shuttle trade secrets to China.* In February 2010, a federal judge in the Central District of California sentenced former Rockwell and Boeing engineer Dongfan "Greg" Chung, 73, of Orange, California, to 188 months in prison for committing economic espionage, acting as an agent of China for more than three decades while employed by Rockwell and Boeing, and making false statements to the FBI. Chung, who had held a "secret" security clearance when he worked at Rockwell and Boeing for more than three decades, misappropriated trade secrets to benefit China, including information related to the Space Shuttle program and the Delta IV rocket. Chung's trial was the first trial under the provisions of the Economic Espionage Act that specifically prohibit theft of trade secrets intended to benefit a foreign government or instrumentality. (CDCA, FBI, NASA).

### (3) Large-Scale Commercial Counterfeiting and Online Piracy

The Department's recent efforts in this area build upon its former initiative in which the Department targeted the 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 websites. In FY2010, the initiative resulted in a number of significant prosecutions, including those set forth below:

- *San Francisco merchants charged with trafficking in millions of dollars worth of counterfeit apparel and accessories.* In August 2010, a 25-count indictment was unsealed charging the owners/operators and several employees of eight shops in San Francisco's Fisherman's Wharf with trafficking in over $100 million of counterfeit merchandise illegally imported from China, including clothing, handbags, wallets, jewelry, watches, sunglasses and shoes from more than 70 well-known designer brands. This law enforcement action, which began in 2007 after CBP intercepted a container of more than $22 million worth of designer accessories, is regarded as the largest enforcement action ever against West Coast retailers. (NDCA, ICE).

- *Two individuals sentenced to prison for conspiring to traffic in counterfeit slot machines and computer programs.* In August 2010, two defendants were sentenced to two years in prison for conspiring to produce and sell counterfeit International Game Technology ("IGT") for video gaming machines and related counterfeit computer programs. Significantly, with assistance from Latvian authorities, one of the defendants was extradited from Latvia, the first individual to be extradited under a new Latvia-U.S. treaty. (CCIPS, DNV, FBI).

- *New York man indicted for trafficking in counterfeit sports jerseys.* In July 2010, Brian Bartoe, 35, of Amherst, New York, was indicted for trafficking in counterfeit goods. Bartoe is accused of selling NFL, NHL, NBA, and MLB counterfeit sports jerseys manufactured in China. Between September 2009 and April 2010, he sold the counterfeit clothing online and at a retail store in Buffalo, New York. The investigation began when CBP intercepted shipments of the merchandise from China that were addressed to Bartoe in Buffalo. (WDNY, ICE, CBP).

- *New York man sentenced to 18 months' imprisonment for selling counterfeit software online.* In May 2010, Robert Cimino, 60, of Syracuse, New York, was sentenced in the Eastern District of Virginia to 18 months in prison for criminal copyright infringement. From February 2006 to September 2009, Cimino generated over a quarter of a million dollars in proceeds by selling pirated copies of popular business, engineering, and graphic design software titles on a variety of Internet-based advertising forums. In addition to his prison term, the court ordered Cimino to pay $272,655 in restitution to copyright owners. (CCIPS, EDVA, FBI).

- *Website operators pled guilty to criminal copyright infringement and to conspiracy to commit criminal copyright infringement.* In March 2010, Robert D. Cook, 56, and Todd A. Cook, 23, both from Wichita Falls, Texas, pled guilty to criminal copyright infringement and conspiracy to commit copyright infringement. The Cooks operated several websites that sold large volumes of downloadable counterfeit software with an estimated retail value of over $1 million. The Cooks' convictions were the latest in an investigation out of Wichita Falls in which four other men have been convicted for operating websites engaged in the sale of pirated software, with a combined retail value of more than $10 million. In October 2010, Todd Alan Cook was sentenced to 18 months in prison and ordered to pay $599,771 in restitution. Robert Cook is scheduled to be sentenced on January 7, 2011. (CCIPS, EDVA, ICE).

- *Washington man indicted for selling almost $2 million in counterfeit Microsoft software.* In February 2010, Wayne Chih-Wei Shu, 44, of Battleground, Washington, was indicted for mail fraud, trafficking in counterfeit goods, and trafficking in illicit labels. Shu is accused of engaging in a ten-year scheme selling counterfeit Microsoft software over the Internet. Shu is alleged to have received over $1.7 million for the counterfeit software from 2004 through 2006. Shu allegedly used counterfeit licenses and certificates of authenticity to fool customers who thought they were purchasing licensed Microsoft products. Shu's trial is scheduled for January 2011. (WDWA, FBI, IRS).

- *Two Kansas men charged with trafficking in counterfeit computer hardware.* In November 2010, Timothy Weatherly, 27, Overland Park, Kansas, pled guilty to conspiracy to smuggle goods into the U.S., to do so by false statements, and to trafficking in counterfeit goods. In December 2009, Weatherly, and his co-conspirator Christopher Myers, 40, of Leawood, Kansas, were indicted for trafficking in counterfeit computer hardware. The indictment alleged that Myers, who in 2003 founded a company called Deals Express, conspired with Weatherly, who in 2005 established a company called Deals Direct, Inc., to import counterfeit Cisco brand computer hardware from China. In August 2005, Weatherly allegedly established a website for Deals Direct and began using eBay to sell counterfeit Cisco products. (DKAN, FBI, ICE).

### (4) Protecting the Marketplace from Domestic and International Organized Criminal Groups

The Department has prosecuted criminal groups and networks whose large-scale online piracy and counterfeiting crimes seriously damage the marketplace for legitimate goods and services.

- *Nine defendants indicted for smuggling millions of dollars in counterfeit goods.* In March 2010, two Malaysian citizens, four Chinese citizens, and three naturalized citizens were indicted on multiple counts arising from a conspiracy to smuggle counterfeit shoes, handbags, wrist watches, and drugs manufactured in China and Malaysia. The defendants were alleged to have smuggled 120,000 pairs of counterfeit Nike shoes, 500,000 counterfeit Coach handbags, 10,000 pairs of Coach and Gucci shoes, and 500 counterfeit Cartier watches through the Port of Baltimore. As part of the takedown, City of London Police arrested six suspects and seized 50,000 items of counterfeit apparel and £350,000 in cash at more than 30 locations. (ICE, CBP, City of London Police, UK Border Agency, DMD).

- *Two defendants convicted by a jury in one of the largest counterfeit goods prosecutions in U.S. history.* In June 2010, two defendants were convicted after a jury trial of importing more than 300,000 fake luxury handbags and wallets worth more than $100 million from China bearing counterfeit trademarks, including those of Burberry, Louis Vuitton, Gucci, Coach, Fendi, Chanel and others in one of the largest counterfeiting luxury goods cases in U.S. history. Defendants organized criminal network involved 13 shell companies and at least eight manufacturing plants in China. At sentencing, the defendants each face a maximum of 30 years in prison and $4.75 million in fines. (ICE, CCIPS, EDVA).

- *Operation in Our Sites I.* On June 30, 2010, ICE agents from the IPR Center executed seizure warrants against nine domain names, executed search warrants on four residences, and seized assets from 15 bank, PayPal and advertising accounts, all related to the operation of commercial movie and television piracy websites. The sites, which earned revenue from advertisements and membership donations, allowed visitors to stream and download hundreds of infringing copies of television shows and pre-release movies, some of which were available days prior to their U.S. theatrical release. Acting on a request for mutual legal assistance, the Dutch National Police seized the server that hosted one of the websites. After the nine domain names were seized, well over 50 million visitors to the websites saw a banner notifying them that the websites had been seized due to criminal intellectual property offenses. (ICE, CCIPS, EDVA, SDNY).

- *Operator of USAWAREZ.COM sentenced to 29 months' imprisonment for criminal copyright infringement.* In April 2010, Richard Humphrey, 22, of North Ridgeville, Ohio, was sentenced to 29 months in prison and to three years of supervised release. Humphrey operated the subscription-based website USAWAREZ.COM, from which he distributed copies of hundreds of pirated movies, computer games and software products. During the investigation, FBI agents seized two personal computers and associated

hardware from Humphrey as well as Humphrey's computer server used to host and run the USAWAREZ.COM website. (CCIPS, NDOH, EDVA, FBI).

- *Two defendants sentenced to 7- and 10-year prison terms for major counterfeit DVD business and public assistance fraud.* In May 2010, Karen Jean Freyling, 48, and Steven Walter Butts, 62, both of Turlock, California, were sentenced, respectively, to 121 months in prison and 94 months in prison for their roles in operating a major Internet-based DVD importation and distribution business as well as for fraudulent receipt of government benefits. The two defendants imported counterfeit DVDs in bulk from suppliers in the Philippines by means of false Customs declarations, and then sold them through websites. Additionally, three employees pled guilty in December 2009 to misdemeanor criminal copyright infringement. (EDCA, FBI, USPIS, CBP, California Employment Development Department, U.S. Social Security Administration)

**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 continues to prosecute such infringers under the Family Entertainment Copyright Act of 2005.

- *Defendant sentenced to 48 months' imprisonment after pleading guilty to criminal copyright infringement and camcording charges.* In June 2010, Brad Newell, 43, of Virginia Beach, Virginia, pled guilty to criminal copyright infringement and the making of an unauthorized recording of motion picture showing in a local theater. Newell was sentenced to 48 months' imprisonment in October 2010. U.S. Immigration and Customs Enforcement ("ICE") agents began investigating Newell and a co-defendant following the receipt of information that Newell and the co-defendant's business engaged in illegally copying and distributing motion pictures. During the investigation, ICE agents seized a video camera used for illegally recording a major motion picture, as well numerous copies of DVDs of that film. (EDVA, ICE)

- *Defendant sentenced after pleading guilty to two counts of unauthorized recording of a motion picture in a motion picture exhibition facility.* In May 2010, Keshawn Deron Wilson, 25, of Asbury Park, New Jersey, was sentenced to six months' confinement, six months' home detention, 400 hours of community service, $14,145 restitution, two years of supervised release and a $200 special assessment following his guilty plea to two counts of "camcording." Wilson was caught in the process of videotaping a major motion picture in a New Jersey movie theater. At the time of Wilson's arrest, authorities seized a high-definition video camera with a 30-gigabyte hard drive. Forensic analysis of the camera revealed a copy of another movie, which Wilson later admitted to recording at the same theater. (CCIPS, MDFL, DNJ, FBI).

***Domestic Training***

During the past year, the Criminal Division provided a number of training programs for federal prosecutors and agents investigating IP crimes. These training courses covered a range of IP enforcement issues and were designed to increase coordination between prosecutors and investigators. Examples of such training included:

- In September 2010, CCIPS organized and taught the Complex Online Crime Seminar at NAC in Columbia, South Carolina. This seminar, which was attended by both prosecutors and federal agents, used a case scenario involving IP crime to provide a number of strategies and techniques for investigating criminal offenses occurring over the Internet.

- In September 2010, the Criminal Division coordinated with the FBI to provide training to FBI Special Agents assigned to investigate IP crimes. The training took place at the IPR Center in Arlington, Virginia.

- In April 2010, CCIPS organized and taught the Intellectual Property Crimes Seminar at the NAC. Both prosecutors and federal agents attended this 3-day course, which included a discussion on the links between IP and international organized crime.

***International Outreach and Training***

The Department of Justice continues to work with other countries to develop effective systems for the enforcement of criminal IP protections. Outreach is accomplished by direct work on specific cases; through extensive cooperation with the State Department and other U.S. agencies -- most notably ICE, CBP and the USPTO -- to provide targeted training and capacity building; through engagement in multi-lateral bodies such as APEC and the Justice Department-led IP Crimes Enforcement Network ("IPCEN") in Asia; and with international law enforcement groups such as the World Customs Organization and INTERPOL.

Recognizing that international IP crime is often interwoven with other criminal conduct, the Department structures training to address the specific issues facing foreign countries or regions, and works to integrate training on topics beyond basic IP crime that will help foreign law enforcement address the problem with the most effective available tools. Examples of this approach from FY2010 include:

- *Attorney General Holder emphasizes the importance of enforcing intellectual property laws to China and a worldwide audience of law enforcement officials.* In October 2010, Attorney General Eric Holder delivered the keynote address at the Fourth Annual International Law Enforcement IP Crime Conference in Hong Kong, which was hosted by INTERPOL and Hong Kong Customs in partnership with Underwriters Laboratory. In attendance at the three-day conference were more than 500 law enforcement agents, prosecutors and industry representatives from approximately forty countries. The Attorney General emphasized the need for transnational cooperation in the investigation and prosecution of intellectual property crimes. Following his trip to Hong Kong, the

Attorney General traveled to Beijing, China where he had a number of meetings with senior law enforcement officials including the Minister of Public Security to stress the importance of IP enforcement and bilateral cooperation between the U.S. and China. Attorney General Holder is the highest-ranking U.S. judicial official to visit China since President Obama took office in 2009.

- *Provided in-depth training on computer forensics to law enforcement authorities from countries in the Asian IP Crimes Enforcement Network in Asia.* This three-day training program, held in December 2009, focused on advanced computer and digital forensics. It was attended by police and prosecutors from four IPCEN nations -- Indonesia, the Philippines, Singapore and Thailand -- and took place at the USPTO's Global Intellectual Property Academy ("GIPA") in Alexandria, VA. It was designed to strengthen international cooperation in fighting large-scale intellectual property theft, disrupt criminal networks that profit from the trade in stolen IP, and enhance cross-border cooperation. Attendees learned to use advanced computer forensics techniques to track down, arrest and prosecute IP criminals. Training was led by the Director of the CCIPS Cybercrime Lab and the IP Law Enforcement Coordinator for Asia. Follow-up programs took place in March 2010 and November 2010 in Singapore and Thailand, and smaller-scale programs have taken place in Mexico, South Africa and regionally in Eastern Europe.

- *Integrating the work of Customs officials and criminal enforcement authorities.* Several programs focused on ensuring greater cooperation between the agencies responsible for identifying and prosecuting large-scale IP smuggling. Successful programs in FY2010 included several border enforcement trainings in Mexico, South Africa and Nigeria, and a pilot program in Ghana to set up an interagency enforcement task force. To continue the success, the Department supported the candidacy of customs officials from South Africa and Mexico in seeking accreditation from the World Customs Organization. These agents will now use their advanced skills to target IP crime and to train other customs officials in their own countries. By increasing the level of communication between seizing agents and prosecutors, the number of criminal investigations generally will also increase. The ultimate goal of these programs is to send smugglers of counterfeit and pirated goods a stronger deterrent message through the imposition of criminal sanctions, which have a greater impact than the economic loss caused by the seizure of an individual shipment of illegal goods.

- *Combating crimes that put the health and safety of the public at risk.* The Department has placed a special emphasis on reducing the traffic of counterfeit products that could harm people. In developing nations where regulatory systems may lag and distribution chains are often compromised, the Department is including segments in its training programs on identifying and disrupting the flow of counterfeit pharmaceuticals. Programs in Mexico during FY2010 for the first time included representatives of COFEPRIS, the Mexican agency with regulatory authority over pharmaceuticals and medical devices, which helped customs officials identify suspicious shipments during trainings at the Port of Manzanillo. Similarly, in March 2010, the Department worked with INTERPOL and regulatory agencies in Tanzania to train more than 100 law

enforcement officials from five East African countries on developing counterfeit pharmaceutical cases.

- *Addressing organized crime through the use of alternate charges.* The Department integrates financial crimes into its training programs. IP crime is usually profit-driven, and the existence of the financial transactions resulting from those IP crimes can provide law enforcement authorities with an avenue to locate and prosecute those responsible. Investigative techniques and criminal statutes used in money laundering, fraud and other white collar cases are often the most effective way to disrupt the production, smuggling and sale of counterfeit and pirated goods, especially in countries where IP statutes do not carry strong penalties or are rarely enforced as stand-alone cases. During FY2010 in Ghana and Senegal, the Department led programs focusing on the development of law enforcement task forces to address IP crime, and included tax investigators and economic crime prosecutors. Ghana and Senegal will use the task force concept to disrupt all facets of the organizations that smuggle counterfeits into those countries. The Department will incorporate and expand this model into programs for other African countries in FY2011.

The design and implementation of international IP training is a time-consuming activity that requires expertise in substantive IP law (both U.S. and foreign) and a detailed knowledge of trends in IP crime. Since 2006, IP training in Asia and Eastern Europe by the Department has often been led by its IPLECs stationed in Bangkok, Thailand and Sofia, Bulgaria. The IPLEC program has been successful at delivering more than 100 tailored training programs to law enforcement officials, and extensive guidance to regional IP policy makers. The IPLEC program has also allowed the Department to provide a greater level of support to international training programs hosted by other agencies in their respective regions. In 2010, the IPLEC program faced substantial transitions, with a new attorney acting as IPLEC/Attaché in Bangkok and the loss of State Department funding for the Eastern European IPLEC. The Department is working to secure permanent funding for the current positions, and to maintain a continuous presence in these critical regions.

In addition to the IPLECs, attorneys from CCIPS planned and executed numerous international training programs using roughly $2 million provided by the State INL and administered by the Office of Overseas Prosecutorial Development, Assistance and Training ("OPDAT"). CCIPS' IP programs have included speakers and subject matter support from many U.S. Attorneys' Offices and other Criminal Division sections, including the OCRS, AFMLS and the Civil Division's Office of Consumer Litigation ("OCL").

As part of the U.S. Government Joint Strategic Plan for IP, the Department has identified countries and regions that will require long-term engagement in training, dialogue and joint operations, and is working with the State Department to secure funding for future training in those priority areas.

***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' Fourth Annual IP Industry/Law Enforcement meeting on June 16, 2010, 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 Attorney General, and senior officials from the FBI, ICE, U.S. Customs and Border Protection ("CBP"), the U.S. Food and Drug Administration ("FDA") and others. More than 90 individuals attended the meeting, including senior representatives from a broad range of industries such as pharmaceuticals, software, luxury goods, electronics, apparel, motion pictures, music, certification mark, consumer goods, and automobiles.

In the past year, the Criminal Division has also organized and hosted training seminars for victims of IP crimes in the New York and Los Angeles areas. 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 (also providing related handouts), as well as some of the ethical limitations placed on prosecutors when evaluating what level and type of assistance can be properly accepted from victims in ongoing prosecutions. The Criminal Division hosted the New York area seminar in November 2009, with participation by the U.S. Attorneys' Offices for the Southern and Eastern Districts of New York and the District of New Jersey. The most recent conference (and 9th in the series) took place in Los Angeles in April 2010. The conference attracted approximately 200 IP rights holders; federal, state, and local law enforcement officials; and federal prosecutors, including the U.S. Attorneys for the Southern and Central Districts of California. A 10th conference is scheduled for January 2011 in Boston.

Through its IP Task Force and CCIPS, the Department maintains two websites that, among other things, provide the public with information on the Department's IP enforcement efforts, assist victims in understanding where and how to report an IP crime, and provide guidance on case referrals. Those links can be found at http://www.justice.gov/dag/iptaskforce/ and www.cybercrime.gov (also linking the IPR Center http://www.ice.gov/iprcenter/iprreferral.htm).

The Bureau of Justice Assistance also partnered with the National White Collar Crime Center to hold a one-day intellectual property crime enforcement summit on September 30, 2010, in Pasadena, CA. The 253 attendees were primarily local and state law enforcement representatives, with many federal law enforcement officials, private company representatives and individuals from academia also present.

### (a)(7)(C) 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 2006 - 2010, listing the number of defendants and cases charged, the number of defendants sentenced, and the length of those sentences.[5] 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 §404(c) of the PRO IP Act, for an accounting of arrest statistics.

As reflected in the chart below, the Department has maintained a relatively consistent number of prosecutions over the course of the last three years. To the extent there is a decrease from FY2008 to FY2010, it parallels the decrease in the number of referrals from investigative agencies. Proportionately, however, the decrease in prosecutions over time has been less significant than the decrease in investigative referrals. Finally, as demonstrated by the cases highlighted above, the Department has also sought to increase the quality and scope of its investigations and prosecutions over the past years, which is not always reflected in statistics. However, given this year's increase in referrals, and the anticipated increase resulting from new investigative resources, the Department anticipates a corresponding increase in prosecutions.

[5] 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 if only a conspiracy to violate one of these offenses was charged.

| District Totals | FY2006 | FY2007 | FY2008 | FY2009 | FY2010 |
|---|---|---|---|---|---|
| **Investigative Matters Received by AUSAs** | 685 | 426 | 365 | 285 | 402 |
| **Defendants Charged** | 339 | 290 | 259 | 235 | 259 |
| **Cases Charged** | 204 | 217 | 197 | 173 | 177 |
| **Defendants Sentenced** | 213 | 287 | 242 | 223 | 207 |
| **No Prison Term** | 106 | 148 | 107 | 126 | 121 |
| **1-12 Months** | 39 | 52 | 48 | 35 | 38 |
| **13-24 Months** | 28 | 37 | 45 | 29 | 27 |
| **25-36 Months** | 14 | 20 | 20 | 6 | 10 |
| **37-60 Months** | 17 | 14 | 19 | 18 | 7 |
| **60 + Months** | 9 | 16 | 3 | 9 | 4 |

### (a)(7)(D) 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 IPR Center, assigning at least one attorney, and sometimes more, to help identify and de-conflict investigative leads, as well as develop and execute national enforcement initiatives. In addition, throughout FY2010, CCIPS detailed a senior prosecutor on a full-time basis to serve as Acting Director to the International Organized Crime Intelligence and Operations Center in Chantilly, Virginia.

The CHIP network consists of more than 230 AUSAs who are specially trained in the investigation and prosecution of IP and computer crimes. The network includes 25 CHIP Units of between two to eight 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. An 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 IPLEC for Eastern Europe will lose its funding from State INL as of March 2011.

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 extensive training on the use of digital forensics tools in IP cases to legal audiences around the world.

Intellectual property enforcement is also an integral part of the mission of three sections of the Department's Civil Division: the Intellectual Property Section, the National Courts Section, and the Office of Consumer Litigation. Through the Civil Division's Intellectual Property Section, the Department assists in initiating civil actions on behalf of CBP to recover penalties imposed by CBP on importers of counterfeit goods and brings affirmative cases when U.S. intellectual property is infringed. The National Courts Section initiates civil actions to recover various penalties or customs duties arising from negligent or fraudulent import transactions, many of which include importation of counterfeit goods. The National Courts Section also defends CBP enforcement of the ITC's Section 337 exclusion orders at the Court of International Trade; these orders are an important tool for patent enforcement. Finally, the Office of Consumer Litigation enforces and defends the consumer protection statutes of the FDA, including the provisions of the Food, Drug, and Cosmetics Act that govern counterfeit drugs and medical devices.

### (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 continues to provide ongoing support to the IPR Center in Arlington, Virginia. Among other things, the IPR Center serves as an investigation clearinghouse for FBI, ICE, CBP, FDA, and others. CCIPS also works closely with the CHIP network to assist in coordinating national prosecution initiatives. Department attorneys will continue to work with the IPR Center to identify and de-conflict investigative leads as well as assist the CHIP network to ensure that investigations and prosecutions are streamlined, not duplicated, and appropriately venued.