United States Department of Justice

PRO IP Act
Annual Report FY2011

Submitted to the United States Congress
December 2011

PRO IP ACT ANNUAL REPORT OF THE ATTORNEY GENERAL FY2011

INTRODUCTION

The Department of Justice (the "Department") submits this 2011 annual 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 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 implementation efforts to implement them during FY2011 (*i.e.*, October 1, 2010 through September 30, 2011) are set forth below.

In February 2010, the Attorney General announced the creation of the Intellectual Property Task Force ("IP Task Force") as part of a Department-wide initiative to confront the growing number of domestic and international IP crimes. The IP Task Force, chaired by the Deputy Attorney General and comprised of senior Department officials from every component with a stake in IP enforcement, has brought a coordinated approach and high-level support to the Department's overall efforts to combat IP crime. 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, which was released in June 2010, as well as the Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations submitted to Congress in March 2011. Although the Department's implementation of the relevant criminal enforcement provisions of the joint strategic plan will be described in the IPEC's upcoming 2011 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 and FY2010, Congress did not appropriate funds in FY2011 for the issuance of state and local law enforcement grants as authorized under Section 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 Section 401 of the PRO IP Act. The FY2011 Intellectual Property Crime 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 on February 10, 2011, and on September 30, 2011, OJP announced that it had awarded approximately $4.9 million in grants to 21 state and local law enforcement agencies and three non-profit organizations in support of the FY2011 Intellectual Property Crime Enforcement Program. Of this $4.9 million, new awards to 13 state and local enforcement agencies totaled approximately $2.5 million, supplemental awards to eight state and local enforcement agencies who had received prior grants totaled approximately $1.5 million, and awards to three non-profit organizations totaled approximately $0.9 million.

The following FY2011 new and supplemental 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 analyses of evidence.

Award Number	Grantee	Amount	New or Supplemental
2011-BE-BX-0005	Bexar County, Texas	$200,000	New
2011-BE-BX-0002	City of Austin, Texas	$200,000	New
2011-BE-BX-0004	City of Central Point Police Department, Oregon	$196,000	New
2011-BE-BX-0003	City of Portland, Oregon	$199,883	New
2011-BE-BX-0007	Cook County State Attorney's Office, Illinois	$178,629	New
2011-BE-BX-0001	County of Marin, Office of the District Attorney, California	$197,980	New
2011-BE-BX-0011	Hartford Police Department, Connecticut	$198,038	New
2011-BE-BX-0009	Los Angeles City Attorney's Office	$200,000	New
2011-BE-BX-0013	Michigan Department of State Police	$200,000	New
2011-BE-BX-0012	New York City Police Department	$200,000	New
2011-BE-BX-0008	Oregon Department of Justice	$191,548	New
2011-MU-BX-0026	San Francisco District Attorney's Office	$198,676	New
2011-BE-BX-0010	Suffolk County District Attorney's Office, New York	$148,102	New
2011-DB-BX-0029	Bronx County District Attorney, New York	$103,022	Supplemental
2011-DB-BX-0017	Los Angeles Police Department	$200,000	Supplemental
2011-DB-BX-0119	Attorney General's Office of Mississippi	$200,000	Supplemental
2011-DB-BX-0013	Los Angeles County Sheriff's Department	$200,000	Supplemental
2011-DB-BX-0130	Chesterfield County, Virginia	$197,690	Supplemental
2011-DB-BX-0020	County of Sacramento, California	$200,000	Supplemental
2011-DB-BX-0021	County of Fresno, California	$200,000	Supplemental

2011-DB-BX-0123	Houston Police Department, Texas	$200,000	Supplemental

As noted above, OJP awarded eight supplemental awards in FY2011 to state and local enforcement agencies who also were recipients of grants in FY2010. Examples of how state and local law enforcement used these FY2010 and FY2011 grants include:

- **Attorney General's Office of Mississippi:** The Mississippi Attorney General's Office launched Operation Knock Out Knock-Offs ("K.O.K.O."), a two-phase statewide effort to combat IP crime. The first phase created a statewide task force, while the second phase focused on consumer and merchant education. In a case arising from one of the K.O.K.O. Task Force's investigations, a store owner and her employee pleaded guilty to selling pirated DVDs out of a retail store front allegedly selling cell phone accessories. In another K.O.K.O. Task Force investigation, more than 100 federal, state, and local agents executed more than 30 federal search warrants across Mississippi in search of counterfeit pharmaceuticals.

- **Chesterfield County, Virginia:** Chesterfield County's Multijurisdictional Special Operations Group ("MSOJ") has partnered with other jurisdictions and industry to take down counterfeiters. For example, in one case, the MSOG, in cooperation with the Richmond Police Department, seized approximately $45,000 in counterfeit clothes and handbags from two Richmond stores. Pirated DVDs, stolen merchandise, and illegal narcotics also were seized.

- **Los Angeles County Sheriff's Department:** Over a two month period (May 2011 to June 2011), the Los Angeles County Sheriff's Department's Counterfeit and Piracy Enforcement team, in conjunction with the Homeland Security Investigations, Immigration and Customs Enforcement – Intellectual Property team, seized over $4 million in counterfeit goods such as software, clothing, and handbags.

In addition, 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"), $250,000:** This supplement to NCPC's FY2009 competitive award and FY2010 supplement supports NCPC's development and implementation of a national IP awareness campaign, the initial phases of which were introduced November 29, 2011.

- **National Association of Attorneys General ("NAAG"), $250,000:** This supplement to NAAG's FY2009 competitive award and FY2010 supplement 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"), $410,432:** This supplement to NW3C's FY2009 competitive award and FY2010 supplement 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 Section 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 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."*

As in FY2009 and FY2010, Congress has not appropriated funds to support Section 402(b) of the PRO IP Act in FY2011.[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 at least two 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.

In addition to the ongoing activities detailed in PRO IP Act Reports for fiscal years 2009 and 2010, the Department has taken the following additional actions to address this important issue:

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. IOC-2 has provided operational, intelligence and financial support to investigations where international organized crime groups were involved in IP offenses.

- The Department made significant contributions to the Administration's Strategy to Combat Transnational Organized Crime ("TOC") released in July 2011 that, among other things, seeks to address organized criminal enterprises engaged in intellectual property

[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."

crime. Also incorporated into that strategy are legislative proposals to strengthen criminal penalties for certain intellectual property offenses. These proposals were first transmitted to Congress as part of the Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations, to which the Department also provided substantial contributions.

Training and Outreach

- In October 2010, the Attorney General delivered the keynote address at the Fourth Annual International Intellectual 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.

- In December 2010, CCIPS, IOC-2, and the Office of Overseas Prosecutorial Development Assistance and Training ("OPDAT") conducted the first African training program in Lusaka, Zambia on investigating organized crime linked to IP crime. The training sought to increase regional cooperation among law enforcement officials from Zambia, Botswana, Tanzania, and Malawi, and among the different agencies involved in organized crime, including customs, financial/tax investigators, IP investigators, prosecutors, and computer forensics specialists.

- In December 2010, representatives from CCIPS and IOC-2 spoke at the First Conference on Organized Crime in Africa in Courmayeur, Italy, about intellectual property perpetrated by organized criminal groups operating out of Africa. The conference was organized by the International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme ("ISPAC") and the National Institute of Justice.

- In December 2010, the Asset Forfeiture and Money Laundering Section ("AFMLS"), the Attorney General's Organized Crime Council ("AGOCC")[2], and the Organized

[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.

Crime and Gang Section ("OCGS") incorporated a training block on the links between IP crime and organized crime at AFMLS/AGOCC/OCGS's Financial Investigations Seminar at the National Advocacy Center ("NAC") in Columbia, South Carolina.

- In March 2011, a CCIPS representative and DOJ prosecutor presented on a panel discussing effective models for international cooperation as a part of the Asian-Pacific Economic Cooperation ("APEC") Dialogue on Corruption & Illicit Trade: Combating Counterfeit (Falsified) Medicines and Strengthening Supply Chain Integrity at the APEC Senior Officials Meeting.

- In March 2011, CCIPS included a training block at the annual Computer Hacking and Intellectual Property ("CHIP") conference on efforts to address organized crime and intellectual property as well as a briefing by IOC-2 on the tools it offers to agents and prosecutors in this area. The conference brought together nearly 200 Assistant U.S. Attorneys ("AUSAs") who specialize in prosecuting high tech crimes and IP crime, and provided 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.

- In May 2011, CCIPS, the FBI, and OPDAT led a workshop on computer forensics and IP crimes for 50 IP and organized crime prosecutors and investigators from various sections of the Mexican Attorney General's Office ("PGR") and the Mexican Federal Police ("SSP") as well as for representatives of IMPI ("Mexican Patent and Trademark Office") who deal with IP enforcement. The workshop brought together prosecutors with their respective digital, financial, and IP division experts and used interactive exercises to provide training on forensic practices and the benefits of enhanced cooperation among these divisions.

- In September 2011, the Thailand Intellectual Property Law Enforcement Coordinator ("IPLEC") and a CHIP prosecutor presented on two panels in a workshop on investigating and prosecuting corruption and illicit trade as part of another APEC Senior Officials Meeting, in which the Consumer Protection Branch ("Consumer Protection") of the Civil Division also participated. The meeting's emphasis was on counterfeit pharmaceuticals.

(a)(5) <u>Authorized Funds Under Section 403</u>

> *"(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 did not receive any authorizations under Section 403 of the PRO IP Act in FY2011.

As noted in the FY2010 PRO IP Act Report, in December 2009, Congress provided funding for the Department to appoint 15 new CHIP prosecutors to support CHIP Units nationwide. The Department was able to fill these 15 new CHIP positions as follows: Northern District of California (2), Central District of California (2), District of District of Columbia, District of Maryland, District of Massachusetts, Eastern District of Michigan, District of New Jersey, Eastern District of New York, Southern District of New York, Southern District of Texas, Eastern District of Virginia, and Western District of Washington. Now that these new CHIP prosecutors are in place, the Executive Office of U.S. Attorneys will monitor data submitted by each district's U.S. Attorney's Office to ensure that these CHIP prosecutors are effectively supporting the Department's intellectual property criminal enforcement initiatives.

The Department may not be able to provide all of the results of the type contemplated in this subsection for several reasons, including the substantial time required to investigate and prosecute an intellectual property crime case and the resulting delay between the placement of the attorneys and the completion of case. Additionally, the Department can retrieve fairly extensive statistical information from its database based on the statute charged (data which is provided as an appendix in the Department's Annual Performance and Accountability Report), but not based on the type of forensic science tool used.

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

(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 did not receive any authorizations under Sections 401, 402 and 403 of the PRO IP Act in FY2011.

(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, CCIPS, and, with regard to offenses arising under the Food, Drug, and Cosmetic Act, the Consumer Protection Branch of the Civil Division. 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 were included in the Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations submitted to Congress in March 2011. Over the course of the past year, the Department also actively participated in a variety of IPEC-led working groups, including those designed to address the proliferation of counterfeit pharmaceuticals online and elsewhere as well as counterfeits in the government's procurement process.

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 260 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 prosecutors 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.

[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. The Department's FY2010 PRO IP Annual Report may be found online at http://www.cybercrime.gov/proipreport2010.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.

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 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.*, National IP Rights Coordination Center ("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

The Department's IP Task Force, which was established by the Attorney General in February 2010, continues to ensure that the Department's IP enforcement strategy and tools are capable of confronting 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

[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; 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.

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 has established three working groups:

- **Enforcement Assessment / Priorities Working Group:** charged with an 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 / International Outreach and Coordination 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, and focuses on expanding international enforcement and capacity building efforts as well as improving relationships with foreign counterparts; and

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

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, IPEC-led working groups, 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 FY2011 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 piracy, particularly occurring online, 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 FY2011, this initiative resulted in a number of significant prosecutions, including those set forth below:

- *Administrator of Florida-based company sentenced to 38 months' imprisonment for her role in sales of counterfeit integrated circuits destined for U.S. military and other industries*. In October 2011, Stephanie A. McCloskey, 39, of Clearwater, Florida, was sentenced to 38 months in prison for her role in a scheme in which she and others imported counterfeit integrated circuits from China and Hong Kong and sold them to the U.S. Navy, defense contractors, and others, marketing some of these products as "military-grade." McCloskey pleaded guilty in November 2010 to a charge of conspiracy to traffic in counterfeit goods and to commit mail fraud. From about January 2007 through December 2009, McCloskey and others generated approximately $15.8 million in gross receipts through their company's sales of counterfeit integrated circuits. (DDC, ICE, NCIS, DOT, USPIS, DCCC, CBP).

- *Two plead guilty to selling counterfeit drugs using Craigslist.* In May and September 2011, Maryland residents Sarah Knott and Dwayne Skiles pled guilty to trafficking in over 45,000 counterfeit Viagra tablets using Craigslist. Both defendants admitted to selling counterfeit drugs from December 2009 through January 2011. Knott and Skiles were each sentenced to two years probation. (DMD, CCIPS, USPIS, FDA's Office of Criminal Investigations ("FDA-OCI")).

- *Belgian citizen sentenced for selling counterfeit, misbranded drugs.* In June 2011, Manuel Calvelo, a Belgian citizen, was sentenced to 48 months in federal prison for his role in operating an Internet pharmacy that sold misbranded and counterfeit drugs as well as controlled substances to consumers in the U.S. and elsewhere. The court also ordered a forfeiture money judgment of more than $850,000 in proceeds. Calvelo, who was arrested in Costa Rica and extradited to Kansas, pleaded guilty to one count of conspiracy to defraud the United States and one count of conspiracy to commit drug trafficking. In

his plea, he admitted that from 2005 to 2008 he and another man operated websites offering for sale more than 40 counterfeit and misbranded drugs. (DKAN, Consumer Protection, FDA-OCI).

- *Chinese national sentenced to over seven years for selling counterfeit weight loss drugs.* In June 2011, Shengyang Zhou, aka "Tom," 31, was sentenced to serve 87 months in prison for trafficking and attempting to traffic in counterfeit versions of the pharmaceutical weight loss drug known as Alli. Additionally, Zhou was ordered to pay over $500,000 in restitution to the victims of his crime, including a Texas emergency room doctor who suffered a mild stroke from ingesting the counterfeit medication. A number of consumers reported feeling an assortment of adverse physical effects from taking the counterfeit Alli that they had purchased from Zhou's webpage or through a re-distributor. Zhou will be deported following his prison sentence. (DCO, FDA-OCI, ICE, USPIS).

- *Florida man indicted for selling counterfeit diabetic test strips.* In May 2011, Jacques Duplessis, 60, of Boynton Beach, Florida, was indicted in the Eastern District of Pennsylvania for his role in a scheme to sell approximately 6,000 boxes of counterfeit LifeScan One Touch diabetic test strips that he purchased from suppliers in China and England. The defendant allegedly sold wholesale quantities to customers in the United States and Canada, who, in turn, sold those counterfeit products to purchasers in pharmacies and other stores throughout the United States. (EDPA, FDA-OCI).

- *Three sentenced to prison for selling lead-tainted counterfeit designer jewelry.* In May 2011, Il Keun Oh, also known as James Ken Oh, 58, and his wife Jacqueline Oh, 56, both of the Hancock Park District of Los Angeles and co-owners of Elegance Fashion Mart, were each sentenced in the Central District of California to 37 months in prison, while Jacqueline Oh's brother, Joon Yeop, 48, of Koreatown, a manager at the store received 30 months' imprisonment, for their respective roles in illegally importing and selling counterfeit designer jewelry. Lab tests revealed that some of the counterfeit products contained nearly 20 times the amount of lead deemed safe by the Consumer Product Safety Commission for handling by children. (CDCA, ICE, CBP, FDIC-OIG).

- *Missouri man sentenced to 46 months in prison for selling counterfeit drugs*. In February 2011, Mark Hughes of St. Louis, Missouri, was sentenced to 46 months in prison for importing and selling counterfeit and misbranded Viagra and Cialis, and also was ordered to pay restitution. Hughes admitted that he sold and ordered more than approximately 11,000 doses of the Viagra and Cialis, which would have had an infringement value of more than $120,000. According to court documents, over an approximately three-year period prior to December 2009, Hughes ordered large quantities of pharmaceutical drugs from sources in India and China without prescriptions for resale. (EDMO, ICE, CBP, USPIS, FDA).

- *Counterfeit pharmaceutical distributor sentenced to 12 months in prison.* In November 2010, Kum Leung Chow, aka Lawrence Chow, 59, was sentenced to 12 months and one day in prison for conspiring to distribute counterfeit pharmaceuticals and trafficking in

pharmaceuticals bearing false labeling and counterfeit trademarks. The investigation revealed that Chow, a Chinese national, used a Hong Kong-based company to obtain and distribute counterfeit Viagra and Cialis pharmaceutical drugs in the United States which he sold over the Internet. Chow sold about 1,120 Viagra tablets and 360 Cialis tablets to undercover ICE-HSI agents over the internet. Shipping documents indicated the drugs were exported from China. (SDTX, ICE, FDA-OCI).

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

In FY2011, 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 11 trade secret cases and two economic espionage cases. Recent cases include:

- *Chinese national pleads guilty to economic espionage and theft of trade secrets from leading agricultural company based in Indianapolis.* In October 2011, Kexue Huang, a 45 year-old Chinese national, pleaded guilty in the Southern District of Indiana to foreign economic espionage and to theft of trade secrets. Huang admitted that during his employment as a research scientist at Dow AgroSciences LLC, he transferred and delivered Dow trade secrets to individuals in China and Germany. With the assistance of these individuals, Huang used the stolen materials to conduct unauthorized research with the intent to benefit foreign universities that were instrumentalities of the Chinese government. Huang further admitted that while working as a biotechnologist for Cargill Inc., he stole one of Cargill's trade secrets, a key component in the manufacture of a new food product. Huang was sentenced to 87 months in prison. (SDIN, DMINN, CCIPS, NSD, FBI).

- *Former Ford engineer sentenced to 70 months for stealing Ford trade secrets*. In April 2011, former Ford employee, Xiang Dong Yu, aka Mike Yu, 49, of Beijing, China, was sentenced to 70 months in prison and ordered to pay a fine of $12,500 for stealing trade secrets from his employer Ford. Yu was a Product Engineer for Ford from 1997 to 2007, and had access to Ford trade secrets, including proprietary design documents. In December 2006, Yu accepted a job at the Beijing Automotive Company. Yu admitted that on the eve of his departure from Ford and before he told Ford of his new job, he copied approximately 4,000 Ford documents onto an external hard drive, including sensitive and highly valuable Ford design documents, and took them to his new employer in China. (EDMI, FBI).

- *Former Goldman Sachs computer programmer sentenced to 97 months for stealing Goldman's trade secrets.* In March 2011, Sergey Aleynikov, 40, of North Caldwell, New Jersey, a former computer programmer at Goldman Sachs & Co. was sentenced to 97 months in prison for theft of trade secrets and interstate transportation of stolen property. Aleynikov was convicted by a jury in December 2010 for stealing from Goldman Sachs proprietary computer code valued at $500 million to benefit his new employer.

Aleynikov was employed by Goldman Sachs from May 2007 to June 2009 as a computer programmer responsible for developing computer programs supporting the firm's high-frequency trading on various commodities and equities markets. On the last day of his employment, Aleynikov transferred substantial portions of the firm's proprietary computer code for its trading platform to an outside computer server in Germany. (SDNY, FBI).

- *Former Dow engineer convicted for conspiring to steal trade secrets.* In February 2011, a federal jury in Baton Rouge, Louisiana convicted Wen Chyu Liu, aka David W. Liou, 74, of one count of conspiracy to commit trade secret theft and one count of perjury. Liu came to the United States from China for graduate work, and worked for the Dow Chemical Company from 1965 until 1992. While employed at Dow, Liu worked as a research scientist on various aspects of the development and manufacture of Dow's elastomers, including chlorinated polyethylene ("CPE"). The evidence at trial established that Liu conspired with at least four current and former Dow employees to misappropriate trade secrets related to Dow's CPE process and product technology. Sentencing is scheduled for January 12, 2012. (MDLA, CCIPS, FBI).

- *Former chemist sentenced to 15 months' imprisonment for stealing trade secrets valued up to $20 million.* In December 2010, David Yen Lee, a former chemist for a paint manufacturing company, was sentenced to 15 months in prison for theft of trade secrets. Lee admitted 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 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. (NDIL, FBI).

(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 (*e.g.*, Craigslist, iOffer), and direct sales websites. In FY2011, the initiative resulted in a number of significant prosecutions, including those set forth below:

- *Michigan woman sentenced to two years' imprisonment for selling counterfeit business software.* In August 2011, Jacinda Jones, 31, of Ypsilanti, Michigan, was sentenced to two years in prison for selling over 7,000 copies of pirated business software with a retail value of over $2 million. She was also ordered to serve three years of supervised release and to pay $441,035 in restitution. Jones illicitly earned more than $400,000 by selling pirated software owned by companies such as Microsoft, Adobe, Intuit, and Symantec through the website www.cheapdl.com. (EDMI, CCIPS, ICE).

- *Maryland man pleads guilty to copyright infringement.* In July 2011, Clarence Matthews, 42, of Upper Marlboro, Maryland, pleaded guilty to criminal copyright

infringement. In his plea agreement, Matthews admitted that beginning no later than August 2006 he advertised television shows and movies for sale on a website. Between August 2006 and March 2011, he collected more than $632,971 in proceeds from the sale of pirated DVDs. The total retail value of all of the copyrighted DVDs that Matthews sold was between $1 million and $2.5 million. During the investigation, law enforcement seized over 44,000 counterfeit DVDs and 19 DVD burner towers from Matthew's residence. Sentencing is scheduled for January 6, 2012. (DMD, FBI).

- *Four plead guilty to conspiracy to distribute pirated DVDs.* In July 2011, four Tennessee individuals, Richard and Melissa Arnold of Hampton, Tennessee; Kristen Bailey, of Erwin, Tennessee; and Reginald Garner of Johnson City, Tennessee, pleaded guilty for their roles in a conspiracy to commit copyright infringement by copying and distributing pirated DVDs. In addition to the counterfeit DVD conspiracy, Richard Arnold also pleaded guilty to making false statements to the Social Security Administration in connection with his receipt of disability benefits. Reginald Garner was sentenced to five years probation. Sentencing is scheduled for February 8, 2012 for Richard Arnold and February 21, 2012 for Melissa Arnold and Kristen Bailey. (EDTN, FBI, SSA-OIG, Carter County Sheriff's Office).

- *Cincinnati man pleads guilty to selling more than $1 million in counterfeit tax preparation software.* In June 2011, Brandon C. Davis, 31, of Cincinnati, pleaded guilty to one count of mail fraud, one count of copyright infringement and two counts of filing a false income tax return for his role in selling more than $1 million worth of counterfeit financial and tax preparation software through an Internet auction site. Davis admitted that he made unauthorized copies of Quicken and Turbo Tax software manufactured by Intuit Inc., which he then sold on eBay. Davis also agreed to a money judgment and tax lien of $80,074, restitution in an amount to be determined by the court, and forfeiture of all computer items used to manufacture and distribute the fake software, a 2006 Hummer and $192,117 that was seized from his bank accounts. Sentencing is scheduled for January 26, 2012. (CCIPS, SDOH, IRS-CI, USPIS, FBI).

- *New Jersey man sentenced to five years in prison for his role in scheme to traffic in counterfeit goods and to bribe port officials.* In January 2011, Michael Hanna, 29, aka "Mike Nova" and "George Flores," of Little Ferry, N.J., was sentenced to five years in prison for his role in a conspiracy to bribe CBP officials with more than $700,000 to traffic counterfeit luxury goods through the Port of Newark and other U.S. ports. Hanna pleaded guilty in March 2010. Hanna admitted that from June 2008 to March 2009, he conspired with others to import counterfeit luxury handbags, pocketbooks, sneakers and other counterfeit goods bearing fake trademarks from legitimate manufacturers such as Coach, Chanel, Gucci, Louis Vuitton, and Nike. He also admitted that over a period of time he paid more than $700,000 in cash to an undercover law enforcement agent whom he believed was acting at the direction of a corrupt CBP official. Hanna made the cash payments to solicit the help of port officials in ensuring that at least 15 of the shipping containers holding the counterfeit merchandise were not seized or detained at port. (DNJ, ICE, CBP).

- *Ohio man sentenced to 30 months in prison for selling thousands of infringing videogames over the Internet.* In December 2010, Qiang "Michael" Bi, 36, of Powell, Ohio, was sentenced to 30 months' incarceration for selling over 35,000 infringing copies of computer games over the Internet with an estimated retail value of $700,000. From 2005 through 2009, Bi sold the infringing copies on eBay.com and Amazon.com and also set up a website for customers to download the games they bought. Bi forfeited $367,669 in cash which represents the proceeds of the crimes, as well as his interests in his house, a car, and all computer and electronic equipment used to illegally copy and sell the games. (SDOH, USPIS, FBI).

- *Virginia man sentenced to 48 months' imprisonment for pirating copyrighted movies.* In October 2010, Brad Newell, 43, of Norfolk, Va., was sentenced to 48 months in prison for pirating and distributing copyrighted movies and for illegally filming or "camming" a movie shown in a local theater. Newell and Nicholas Skamagos opened and operated "Burn Central" from a Norfolk storefront. Burn Central specialized in selling DVDs containing pirated copies of copyrighted movies that had not yet been released to DVD. Newell's business partner, Nicholas Skamagos, and a Burn Central employee, Kiah Fields, previously pled guilty and were sentenced to six and five months, respectively, for their roles in the illegal activities conducted at Burn Central. (EDVA, ICE).

- *Operation in Our Sites v. 2.0.* On November 29, 2010, on "Cyber Monday," which is known as the busiest online shopping day of the year, agents executed seizure orders against 82 Internet domain names of domestic and international businesses selling a diverse array of counterfeit and pirated goods. The operation disrupted the sale of thousands of infringing items and redirected those seeking to access the illegal websites to a banner containing a notice that law enforcement seized the domain names for counterfeiting and piracy. *Operation In Our Sites* is an ongoing initiative seeks to seize domain names associated with websites that distribute pirated and counterfeit goods. The owners of these websites are usually located overseas and therefore are unlikely ever to be brought to the United States to face charges. (CCIPS, AFMLS, SDNY, DDC, MDFL, DCO, SDTX, CDCA, NDOH, DNJ, WDWA, 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.

- *Three Mexican nationals sentenced for conspiring to use forced labor for pirated CD/DVD sales.* In October 2011, Estela Aguilar-Lopez, 47, Blanca Estela Lopez-Aguilar, 37, and Francisco Ivan Rodriguez-Garcia, 29, were sentenced to 46, 50, and 57 months in prison, respectively, for conspiring to force labor and conspiracy to distribute copyrighted works. Aguilar-Lopez, Lopez-Aguilar, and Rodriguez-Garcia previously pled guilty to these charges in March 2011. Aguilar-Lopez, Lopez-Aguilar, and Rodriguez-Garcia used undocumented aliens to distribute copyrighted materials on CD

and DVD as payment for the defendants' assistance to the aliens in entering the United States. The FBI investigation revealed that the defendants abused the undocumented aliens verbally and physically, using threats of force and force to compel the service of the undocumented aliens until their debts were paid. (SDTX, FBI, Harris County Sheriff's Office, ICE-HSI, State DSS, Texas Attorney General's Office as part of the Human Trafficking Rescue Alliance (HTRA)).

- *Founders of NinjaVideo plead guilty to criminal copyright conspiracy.* In September 2011, two Ninjavideo co-founders, Matthew David Howard Smith, 23, of Raleigh, NC, and Hana A. Beshara, 29, of Las Vegas, NV, pleaded guilty to conspiracy and criminal copyright infringement, and in November 2011, co-founder, Justin A. Dedemko, 28, of Brooklyn, NY, pleaded guilty to conspiracy to commit copyright infringement. The website, NinjaVideo.net, provided millions of users with the ability to illegally download copyright-protected movies and television programs in high-quality formats. NinjaVideo generated over $500,000 in income from Internet advertising and visitor donations during the course of the conspiracy. Additionally, in October 2011, one of NinjaVideo's main uploaders, Joshua David Evans, 34, of North Bend, WA, pleaded guilty to conspiracy and criminal copyright infringement. Also in October 2011, Jeremy Lynn Andrew, 33, of Eugene, OR, who served as head of security for NinjaVideo.net pleaded guilty to conspiracy. An arrest warrant has been issued for the last remaining indicted co-conspirator, Zoi Mertzanis, 36, of Greece. Sentencings will be held on January 6, 2012 for Beshara; January 20, 2012 for Smith; January 27, 2012 for Evans; February 3, 2012 for Andrew; and February 24, 2012 for Dedemko. (EDVA, CCIPS, ICE).

- *Seven indicted for extensive counterfeit media operation.* In September 2011, Leonel Martinez Caballero, 28; Vincenta Munoz-Peralta, 38; Mariano Vega Hernandez, 24; Roman Santana, 28; and Edgar Alonso Bautista Arazate, 30; all of Modesto, California; Martin Munoz Peralta, 39, of San Jose; and Antonio Hernandez Sanchez, 27, of Stockton, were all charged with criminal copyright infringement, trafficking in counterfeit labels, and conspiracy to commit these offenses. According to the indictment, Caballero managed a warehouse in Modesto that served as a distribution point for counterfeit CDs and DVDs. The investigation revealed that in July 2011 the warehouse contained over 100,000 counterfeit CDs and DVDs. The indictment also alleged that a counterfeit DVD manufacturing operation was being operated out of Caballero's rented residence. His co-conspirators purchased large amounts of counterfeit media from the warehouse for resale to the public. (EDCA, FBI, Sacramento Valley Hi-Tech Crimes Task Force).

- *Woman sentenced to 60 months in prison and man sentenced to 30 months in prison for importing and selling counterfeit Cisco equipment.* In September 2011, Chun-Yu Zhao, 43, of Chantilly, VA, was sentenced in the Eastern District of Virginia to five years in prison for leading a conspiracy to import and to sell counterfeit Cisco-branded computer networking equipment, laundering criminal proceeds and fraudulently obtaining her citizenship. Zhao and her family members and other co-conspirators in China used counterfeit labels and packaging to mislead consumers into believing that they were purchasing genuine Cisco products. Zhao also was ordered to pay over $2.7 million in restitution and a $17,500 fine. Additionally, Zhao's U.S. citizenship has been revoked.

Zhao's four homes in Maryland and northern Virginia and three condominiums in Chantilly totaling more than $2.6 million, a Porsche Boxster, Porsche Cayenne, Mercedes sedan, and her seven bank accounts containing more than $1.6 million all have been forfeited to the United States. In August 2011, co-conspirator Donald H. Cone, 48, of Frederick, Maryland, was sentenced 30 months in prison for his role in the conspiracy, and was ordered to pay $148,300 in restitution. (EDVA, CCIPS, ICE, GSA-OIG).

- *Five CD and DVD counterfeiters and suppliers in Atlanta sentenced to prison.* In February 2011, four individuals were sentenced in Atlanta for their involvement in a counterfeit DVD and CD ring, and in June 2011, one individual was sentenced for his involvement in the same ring. In February 2011, Mamadou Sadio Barry, 40, was sentenced to 60 months in prison; Moussa Baradji, 29, was sentenced to 50 months in prison; Sedikey Sankano, 42, was sentenced to 24 months in prison; and Won Ahn, 69, was placed on probation for one year. In June 2011, Ibrahim Diallo, 27, was sentenced to 38 months in prison. The court found that these defendants were responsible for distributing illegal copies of products that, if legitimate, would have been valued at more than $2 million. The sentenced defendants were among 13 charged by a federal grand jury in May 2009, in an indictment alleging various copyright, trademark and counterfeit goods offenses. The case is one of the largest copyright piracy prosecutions in the southeast. (NDGA, CCIPS, FBI, ICE, Atlanta Police Department Organized Crime Unit, College Park, Ga. PD, East Point, Ga. PD).

Domestic Training

During the past year, the Department provided a number of training programs for federal, state, and local 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 as well as coordination between federal, state, and local law enforcement agencies. Examples of such training included:

- Throughout FY2011, the Criminal Division coordinated with the IPR Center's IP Theft Enforcement Team ("IPTET") to provide training to ICE agents, CBP officers, and state and local law enforcement agents across the county. These training sessions took place in Detroit, Michigan (March 2011), Minneapolis, Minnesota (May 2011), Houston, Texas (June 2011), and Tampa, Florida (August 2011).

- In August 2011, CCIPS organized and taught the Complex Online Crime Seminar at the 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 June 2011, CCIPS organized and taught the Electronic Evidence and Basic Cybercrime Seminar at the NAC in Columbia, South Carolina. This seminar, which was attended by primarily prosecutors, taught students the basics of the Internet, e-mail, computer forensics, drafting search warrants, using electronic evidence in court, and

international issues. Additionally, students were trained in charging and prosecuting intellectual property, computer crime, and fraud offenses.

- The Bureau of Justice Assistance ("BJA") partnered with the National White Collar Crime Center and the National Association of Attorneys General to offer law enforcement personnel and prosecutors a series of one-day training seminars entitled "Fake Products, Real Crime: Intellectual Property Theft." These seminars were held across the country throughout FY2011 in locations such as Durham, North Carolina; Baldwin Park, California; Denver, Colorado; and Rye Brook, New York. The goal of these seminars was to increase the quantity and quality of investigations and prosecutions of IP crime by state and local law enforcement.

CCIPS had planned to conduct two additional intellectual property training seminars at the NAC in FY2011 for prosecutors and federal agents, including the Trade Secrets/Economic Espionage Seminar and the Intellectual Property Crimes Seminar, however those seminars were canceled due to a lack of funding.

International Outreach and Training

The Department continues to work with law enforcement counterparts around the world to address the growth of IP crime as an international phenomenon. The Department seeks to engage foreign law enforcement through meetings of officials ranging from the Attorney General to line attorneys and agents in order develop the expertise and will to address IP crime at its source.

Attorney General Holder set the tone for DOJ's international activities in FY2011, when he addressed an audience of over 500 investigators, prosecutors and rights holders at the International Law Enforcement IP Crime Conference in Hong Kong, immediately followed by a visit to China in October 2010, when he met with Chinese Ministry of Public Security officials to discuss the critical importance of cooperation and joint investigations to reduce the production, smuggling, and sale of counterfeit and pirated goods emanating from China.

CCIPS and OPDAT worked with State Department grants and in cooperation with other U.S. agencies in 2011 to provide training to foreign officials on effective enforcement of IP laws. CCIPS' IP training is designed to increase cooperation between various law enforcement agencies with responsibility for IP offences, to utilize various types of charges, including economic and organized crime statutes to get at IP crime, and to increase the knowledge of enforcement officials and the judiciary about the importance of reducing counterfeiting and piracy.

Major ongoing initiatives in Mexico and on the African continent continued in 2011, as highlighted:

MEXICO

Computer Forensics and IP Crimes, Mexico City, Mexico (June 2011)

The program brought together 50 IP and organized crime prosecutors and experts from the Digital, Financial and IP divisions of the Mexican Attorney General's Office ("PGR"), as well as representatives from the Mexican Patent and Trademark Office ("IMPI") to discuss computer forensic practices and enhance the working relationship among these disparate groups when it comes to electronic evidence. Following the program, the prosecutors and investigators indicated that they now possess a greater understanding of the importance that electronic evidence plays in IP crimes, where to turn for issues of electronic evidence, and how to ask relevant questions on electronic evidence in their cases.

Criminal Enforcement of IP at the Border, Manzanillo, Mexico (July 2011)

In this program, DOJ worked with several agencies including the World Customs Organization, U.S., and Mexican right holders (including the U.S. Chamber in Mexico), and the various IP agencies in Mexico (Aduanas—the Mexican customs service), IMPI, and Indautor (the Copyright Office) to provide a new generation of Mexican officials the skills necessary to identify counterfeit products, to refer cases for criminal prosecution, and to continue to establish prosecutors at the major ports in Mexico. Based on the past success of similar programs the Mexican Navy requested to participate to increase interagency cooperation on enforcement. The training resulted in participants identifying containers of counterfeit products which led in turn to new criminal investigations.

SUB-SAHARAN AFRICA

9th Interpol IP Crime Training Seminar, Lagos, Nigeria (June 2011)

In this program, DOJ used its experience in Nigeria to assist Interpol in exploring for the first time, how to engage different Nigerian agencies that have partnered with DOJ on IP enforcement in the past, namely, Nigerian Police, Economic and Financial Crimes Commission ("EFCC"), Nigerian Customs Service ("NCS"), Nigerian Copyright Commission ("NCC"), National Agency for Food and Drug Administration and Control ("NAFDAC"), and Standards of Nigeria ("SON"). As a result of the program, different follow-up activities are now planned for later in 2012 among Nigerian law enforcement, Interpol and DOJ.

Enforcement of IP Rights in Kenya: An Interagency Approach, Nairobi, Kenya (May 2011)

DOJ worked with Commercial Law Development Program ("CLDP") of the Commerce Department and the U.S. Embassy in Nairobi, to organize a four-day regional workshop that exposed 70 enforcement officials from Kenya and across the East Africa region to best practices in interagency collaboration on IP enforcement. The workshop provided guidance as the Kenyan Anti-Counterfeiting Agency ("ACA") and the Kenyan partner agencies determined the mechanisms and procedures for cooperation, collaboration, and communication as they establish

the most effective approach to fighting trade in counterfeit and pirated goods. It also included substantial training on public-private sector coordination, training on product identification and customs recordation. By promoting an interagency approach among the key partner agencies and the private sector, the workshop helped to establish an effective framework and mechanisms by which counterfeited and pirated goods can be prohibited from entering Kenya and removed from Kenya's markets.

Role of the Judiciary in the Enforcement of IP Rights, Kigali, Rwanda (June 2011)

The Department, CLDP, and the Federal Judiciary worked together to organize the first regional DOJ Workshop in East Africa for the judiciary on IP enforcement. Tanzania, Kenya, Burundi, Rwanda, and Uganda were represented. The event helped to develop the quality of IP protection in Rwanda and in the East African Community ("EAC") by improving the skill and knowledge level necessary to provide fair, efficient, and consistent adjudication of IP cases based upon the standards of protection afforded by the EAC, its member countries, and international law. At the conclusion of the event, the participating judges decided to share judicial opinions in IP cases, to work with the legislative branches of their respective countries to review existing statutes to ensure that issues raised by current technologies and other contemporary threats are deterred sufficiently. The participants also agreed to ensure that in enforcement additional non-IP criminal tools should be brought to bear to deter IP violations, including asset forfeiture, money laundering, fraud, non declaration of currency, criminal customs laws, building code violations, etc.

African Global Intellectual Property Academy (August 2011)

With USPTO and CLDP, DOJ organized "Consultations on an Interagency Approach to the Enforcement of Intellectual Property Rights" at the USPTO 2011 African Global Intellectual Property Academy ("GIPA"). Twenty-five police, prosecutors, health and safety, patent, trademark, copyright and customs officials from Kenya, Nigeria, Liberia, and Ghana attended. As a result of the GIPA, the participants indicated that they now better understood the importance that interagency cooperation plays in criminal IP enforcement, as well as some of the developing challenges that African countries face in criminal IP enforcement due to the digital environment, especially with the rapid growth of mobile telephone banking and payment, which may significantly complicate the detection of financial transactions involving counterfeiters.

In addition to these DOJ-led programs, Department attorneys provided significant assistance in numerous training programs provided by other agencies, including:

- Worked with the U.S. Patent and Trademark Office and the U.S. Embassy to provide IP and digital piracy training for judges and law enforcement officials in Delhi, Kolkata, and Mumbai over a ten-day span in September 2011;
- Trained judges, prosecutors and customs officials in Asuncion, Paraguay in a State Department sponsored four-day program in June 2011. The training provided case study examples on copyright and trademark counterfeiting and guidance on obtaining evidence from foreign countries;

- Assisted the staff of the International Law Enforcement Academy ("ILEA") in El Salvador conduct a week-long training in March 2011 for prosecutors and law enforcement officials specializing in IP cases from Belize, Guatemala, Mexico, Panama and the host country;
- Co-hosted the ASEAN-USPTO-USDOJ Workshop on Copyright and Effective Practices Against Digital and Internet Piracy in Bangkok, Thailand in March 2011. More than 50 IP enforcement officials from nine countries heard DOJ speakers provide training on Internet piracy, using financial investigation techniques in IP cases, and guide a mock trial of a criminal IP trial;
- Provided input and speakers from the Civil and Criminal Divisions to the APEC Counterfeits in the Illicit Trade meetings held during the course of the year; and
- Participated in more than 15 programs in seven countries in Asia through the DOJ IP Law Enforcement Coordinator for Asia.

Unfortunately, FY2011 saw the termination of State Department support for the Eastern European IP Law Enforcement Coordinator program. During his posting in Sofia, Bulgaria, DOJ's Eastern European IPLEC was responsible for more than 100 IP-specific training programs and countless consultations and technical guidance on IP enforcement issues. In the proposed FY2012 administration budget, there is a request for funds for International Computer Hacking and Intellectual Property ("ICHIP") coordinators, who would take on the training and operational responsibilities for international IP enforcement and provide additional guidance in the area of cyber crime and electronic evidence on behalf of the Department.

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' Fifth Annual IPR Industry/Law Enforcement meeting on July 22, 2011, 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 Assistant Attorney General Lanny Breuer. Senior law enforcement officials from the FBI, ICE, U.S. Customs and Border Protection ("CBP"), and FDA-OCI participated in the meeting. More than 80 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's high-level officials and CCIPS attorneys have also presented at a variety of domestic and international conferences, symposiums and workshops attended by IP rights holders and law enforcement officials. These events included: International Anti-Counterfeiting Coalition's Fall Conference in Scottsdale, Arizona in October 2010; Global Conference on Combating Counterfeiting and Piracy in Paris, France in February 2011; International Anti-Counterfeiting Coalition's Spring Conference in San Francisco, California in May 2011; Underwriters Laboratories Brand Protection Summit in San Diego,

California in June 2011; International Law Enforcement IP Crime Conference in Madrid, Spain in September 2011; and the IPR Center Intellectual Property Symposium in Arlington, Virginia in September 2011.

Notably, in September 2011, Assistant Attorney General Lanny Breuer provided keynote remarks on the first day of the 2011 International Law Enforcement IP Crime Conference held in Madrid, Spain. The conference, entitled "Transforming Regional Success into Global Action," brought together over 400 law enforcement and customs personnel from 50 countries to gain an international perspective on the trade in counterfeit and pirated products; to share international best practices on how to effectively combat this illegal trade; and to provide a global forum for networking and partnership development.

In past years, the Criminal Division has organized and hosted regional training seminars for victims of IP crimes in variety of areas across the country. 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. Due to a lack of funding, the Criminal Division was not able to organize and host any of these seminars in FY2011.

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 http://www.cybercrime.gov/ (also linking the IPR Center http://www.ice.gov/iprcenter/iprreferral.htm).

In addition, the Department is working with the National Crime Prevention Council on a public awareness campaign in order to help educate the public about IP crime and its consequences, the initial phases of which were introduced November 29, 2011.

Additionally, in conjunction with the BJA National Conference, OJP and BJA held a half-day IP theft forum on December 8, 2010, in Washington, D.C., entitled "Buying Fake Bags, Medicine and Music: Good Bargain or Deadly Investment? What you Need to Know About Intellectual Property Crime." Representatives from industry and national organizations as well as state and local law enforcement attended the forum, which addressed the health and safety risks posed by counterfeit products, the damaging efforts of IP crime on the economy, and the relationship of IP crime to gangs and organized crime. The forum also emphasized the importance of federal, state, and local law enforcement coordination in aggressive IP law enforcement.

(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 2007 - 2011, 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 Section 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 FY2009 to FY2011, 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. In addition, the number of defendants receiving sentences in excess of 12 months has increased from FY2010 to FY2011. 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 FY2010 and FY2011's increase in referrals, the Department anticipates a corresponding increase in prosecutions.

District Totals	FY2007	FY2008	FY2009	FY2010	FY 2011
Investigative Matters Received by AUSAs	426	365	285	402	387
Defendants Charged	290	259	235	259	215
Cases Charged	217	197	173	177	168
Defendants Sentenced	287	242	223	207	208

[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.

No Prison Term	148	107	126	121	102
1-12 Months	52	48	35	38	27
13-24 Months	37	45	29	27	33
25-36 Months	20	20	6	10	17
37-60 Months	14	19	18	7	21
60 + Months	16	3	9	4	8

(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, when fully staffed. 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 FY2011, 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 260 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 a Department attorney in Bangkok, Thailand, who handles IP issues in Asia. An IPLEC for Asia has been stationed in Bangkok since January 2006. From November 2007 until March 2011, when the IPLEC for Eastern Europe lost its funding from State INL, a Department attorney served in Sofia, Bulgaria, in order to handle IP issues in Eastern Europe. The President's proposed budget for FY2012 contains a request to permanently fund Department positions to address IP and cybercrime issues overseas.

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 Consumer Protection Branch. 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 Consumer Protection Branch conducts civil and criminal litigation under the Food, Drug, and Cosmetic Act, including prosecuting counterfeit drug and medical device offenses.

(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.