United States Department of Justice

PRO IP Act
Annual Report FY2013

PRO IP ACT ANNUAL REPORT OF THE ATTORNEY GENERAL FY 2013

INTRODUCTION

The Department of Justice (the "Department") submits this Fiscal Year 2013 ("FY 2013") 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 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. Those provisions and the Department's implementation efforts to implement them during FY 2013 (*i.e.*, October 1, 2012 through September 30, 2013) 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 Enforcement Coordinator ("IPEC"), the Department contributed to the 2013 Joint Strategic Plan on Intellectual Property Enforcement (June 2013), the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets (February 2013), the Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations (March 2011), and the IPEC's annual reports, among other things. The Department also participates in a number of IPEC-led working groups.

(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."*

In FY 2013, Congress appropriated funds for the first time for the issuance of state and local law enforcement grants as authorized under Section 401 of the Act. The Office of Justice Programs ("OJP") awarded grants to support state and local IP law enforcement task forces and local IP training and technical assistance as authorized by the Consolidated and Further Continuing Appropriations Act, 2013 (Intellectual Property Enforcement) Pub. L. No. 113-6, 127

Stat. 198, 253 and as informed by Section 401 of the PRO IP Act. The FY 2013 Intellectual Property Enforcement Program ("IPEP"), 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 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 United States Attorneys' Offices. The information shared under the program includes 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 ("BJA"), a component of OJP.

In September 2013, OJP announced that it had awarded $2,190,308 in grants to eleven state and local law enforcement agencies in support of the FY 2013 IPTEP. OJP awarded new grants to five jurisdictions that had achieved high scores in the FY 2012 competitive process for the IPEP, [1] but did not received grants that year due to budget constraints. OJP awarded six supplemental awards in FY 2013 to state and local enforcement agencies who also were recipients of grants in FY 2010, 2011, or 2012. The following FY 2013 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, forensic analyses, and prosecutions; and acquiring equipment to conduct investigations and forensic analyses of evidence.

Award Number	Grantee	Amount	New or Supplemental
2013-ZP-BX-0010	City of Los Angeles (Los Angeles Police Department)	$200,000	New Award to Unfunded FY 2012 Applicant
2013-ZP-BX-0005	Mississippi Attorney General's Office	$188,775	New Award to Unfunded FY 2012 Applicant
2013-ZP-BX-0003	New York City Police Department	$200,000	New Award to Unfunded FY 2012 Applicant
2013-ZP-BX-0002	Suffolk County District Attorney's Office	$200,000	New Award to Unfunded FY 2012 Applicant

[1] Although Congress did not appropriate funds in FY 2010, 2011, or 2012 for the issuance of state and local law enforcement grants as authorized under Section 401 of the Act, OJP offered competitive grants to support state and local law enforcement IP task forces and local IP training and technical assistance, as authorized by general funding bills (e.g., the Consolidated and Further Continuing Appropriations Act of 2012 (P.L. 112-55)) and informed by Section 401 of the PRO IP Act.

2013-ZP-BX-0014	Cook County State's Attorney's Office	$213,300	New Award to Unfunded FY 2012 Applicant
2013-ZP-BX-0008	City of Los Angeles (Los Angeles City Attorney's Office)	$200,000	Supplement to Previous Award
2013-ZP-BX-0006	City of Houston	$200,000	Supplement to Previous Award
2013-ZP-BX-0013	Los Angeles Sheriff's Department	$194,118	Supplement to Previous Award
2013-ZP-BX-0017	Bronx County District Attorney's Office	$194,115	Supplement to Previous Award
2012-DG-BX-0012	Cook County Sheriff's Office	$200,000	Supplement to Previous Award
2013-ZP-BX-0034	North Carolina Department of the Secretary of State	$200,000	Supplement to Previous Award

Since the inception of the program, state and local law enforcement have seized $251,759,893 in counterfeit merchandise; $16,813,323 in other property, and $3,206,166 in currency (total aggregate seizure value: $271,779,383). In addition to these seizures, grantees achieved the following in the one-year period from July 1, 2012 to June 30, 2013:

- 1,230 individuals were arrested for violation of IP laws;
- 232 state and local IP search warrants were served; and
- 381 piracy/counterfeiting organizations were disrupted or dismantled.

BJA also continues to support one-day training events on IP rights for state and local law enforcement agencies across the country through cooperative agreements with the National White Collar Crime Center ("NW3C") and National Association of Attorneys General. In FY 2013, these training sessions took place in Topeka, Kansas; Fayetteville, Arkansas; Charleston, South Carolina; Burlington, Kentucky; Burbank, California; Allison Park, Pennsylvania; Phoenix, Arizona; Albany, New York; Sandusky, Ohio; Omaha, Nebraska; Cape Elizabeth, Maine; Manassas, Virginia; Bismarck, North Dakota; Sandy, Utah; and Philadelphia, Pennsylvania. NW3C also conducted several tailored seminars as well as engaged in additional technical assistance visits to grantee agencies in order to improve their IP investigative and prosecutorial approaches. In FY 2013, BJA awarded an NW3C an additional $907,452 to support the continuation of these important trainings and the expansion of training and technical assistance support to jurisdictions engaged in IP enforcement activities.

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

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

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

(a)(3) <u>FBI Training</u>

> *"(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.

"(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."

(a)(4) Organized Crime Plan

As in FY 2009 through FY 2012, Congress did not appropriate funds to support Section 402(b) of the PRO IP Act in FY 2013.[2] Nevertheless, the Department has continued to take a number of actions, described below, in an effort to implement this provision. The 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 through 2012, 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 (the "Center") in an ongoing effort to develop and implement a mechanism to both contribute data to the Center to address intelligence gaps as they relate to IP, among other things. The Center has provided operational, intelligence, and financial support to investigations where international organized crime groups are involved in IP offenses.

Training and Outreach

- In October 2012, representatives of CCIPS, OPDAT, and INTERPOL organized a

[2] 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 United States 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."

conference entitled "Integrated Criminal Enforcement Training against Trafficking in Illicit Goods" in Dar Es Salaam, Tanzania. The three-day event brought together more than fifty officials from police, prosecutor's offices, customs, intellectual property agencies, as well as intellectual property law enforcement experts from Tanzania and from neighboring countries like Burundi, Uganda, Kenya, Rwanda and Congo. The training included methodology in identifying, targeting, and dismantling transnational organized crime groups involved in the manufacture and distribution of counterfeit goods.

- In April 2013, representatives of CCIPS and OPDAT traveled to Mexico to conduct assessment meetings with representatives of different Mexican agencies that handle issues related to the enforcement of IP crimes, including the head of the organized crime division at the Mexican Attorney General's Office, and the organized crime unit of the Mexican Federal Police. Meetings were also held with witness protection representatives to address how to better protect law enforcement officers who handle IP cases.

(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 which such tools were used."*

As noted in the Department's FY 2012 PRO IP Act Report, in December 2009, the Department selected fifteen new AUSA positions to support CHIP units nationwide with an emphasis on IP enforcement.

FY 2011 was the first full fiscal year during which the additional AUSAs were in place. Between FY 2010 and FY 2011, there was a slight decline in the number of IP enforcement cases and defendants charged. It was anticipated, however, that as the new prosecutors developed experience, their workload statistics, including cases filed, would increase. As reflected in the statistics provided in Section (a)(7)(C) herein, the Department began to see an increase in FY 2012. In FY 2013, however, the number of IP investigative matters received from law enforcement agencies decreased (390 matters in FY 2012 and 334 matters in FY 2013), and there was a corresponding decrease in the number of IP cases opened and defendants prosecuted. In

FY 2012, 178 IP enforcement cases were filed nationwide, with 254 defendants charged. In FY 2013, 163 IP enforcement cases were filed nationwide, with 213 defendants charged. The Department, however, has sought to increase the quality and scope of its investigations and prosecutions over the past years, which is not always reflected in statistics.

In April 2013, CCIPS organized and led the annual CHIP training conference at the National Advocacy Center ("NAC"). The conference brought together over 100 members of the national CHIP coordinators' network 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.

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) <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 did not receive any authorizations under Sections 401, 402 and 403 of the PRO IP Act in FY 2013.

(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 United States 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 is 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 Foreign and Economic Espionage Penalty Enhancement Act of 2012, which increased fines for theft of trade secrets committed with the intent to benefit a foreign entity; the Theft of Trade Secrets Clarification Act of 2012, which clarified that the Economic Espionage Act applies to trade secrets that are "related to a product or service used or intended for use in interstate or foreign commerce"; the National Defense Authorization Act for FY 2012, which enhanced penalties for certain offenses involving "counterfeit military goods"; the Food and Drug Administration Safety and Innovation Act, which created a new offense for "trafficking in counterfeit drugs"; the PRO IP Act of 2008; the Family Entertainment and Copyright Act of 2005, 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, which criminalized the unauthorized reproduction and distribution of copyrighted works without a commercial purpose or financial gain; and the Economic Espionage Act of 1996, which criminalized the theft of trade secrets, including economic espionage.[3]

The Department made substantial contributions to the criminal enforcement proposals contained in the Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations (March 2011), including several of which (described above) that were enacted into law. The Department looks forward to working with Congress as it considers additional proposals.

The Department coordinates closely with IPEC in addressing the Administration's priorities on intellectual property enforcement and actively participates in a variety of IPEC-led working groups, including multi-agency groups designed to address the proliferation of counterfeit pharmaceuticals online and elsewhere, counterfeit goods in the government's procurement process, and the theft of trade secrets by foreign actors.

CCIPS and CHIP Program

The Department carries out its overall IP criminal prosecution mission through the United States Attorneys' Offices and CCIPS, which works closely with a network of over 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 up to 38 prosecutors who are devoted enforcing laws related to computer and IP crimes. Thirteen CCIPS attorneys are assigned exclusively to intellectual property enforcement.

[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://publicdevelopment.doj.gov/dag/iptaskforce/proipact. The Department's FY 2010-FY 2012 PRO IP Reports are available at the same location.

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 criminal enforcement of IP laws to prosecutors and investigative agents both domestically and abroad.

CCIPS continues to place a high priority on fostering international cooperation and coordination of criminal IP enforcement efforts. It has developed relationships with foreign law enforcement through international casework as well as through training and outreach. An important component of the Department's international enforcement efforts is the Intellectual Property Law Enforcement Coordinator ("IPLEC") program. In the current program, the Department has placed an experienced federal prosecutor in Bangkok, Thailand, who handles IP issues in Asia. The Department is also working closely with the State Department to deploy a new IPLEC for Eastern Europe. Additionally, the President's proposed budget for FY 2014 contains a request to expand and enhance the program by permanently funding up to four Department Attachés who would be cross designated as International Computer Hacking and Intellectual Property ("ICHIP") coordinators. The ICHIP Attachés would be deployed in key locations overseas to assist in implementing the Department's international IP and cybercrime mission.

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 United States Attorneys' Offices has at least one CHIP coordinator. In addition, 25 United States Attorneys' Offices have CHIP Units, with two or more 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 evidence; (3) training prosecutors and law enforcement personnel in the region; and (4) conducting public and industry outreach and awareness activities.

CES and the NSCS Network

In 2012, the Department established the National Security Cyber Specialists' ("NSCS") to create a "one-stop-shop" for attorneys, investigators, and members of the private sector looking to combat national security cyber thefts—including economic espionage and trade secret theft—with all appropriate legal tools. Each U.S. Attorney's Office has at least one

[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.

representative to the NSCS Network. That representative provides technical and specialized assistance to his or her colleagues within the relevant U.S. Attorneys' Offices and serves as a point of contact for coordination with the Department's headquarters. At headquarters, all National Security Division ("NSD") components, CCIPS, and other relevant sections of the Criminal Division are members of the Network. The Department relies on the NSCS Network to disseminate intelligence and other information to the field, to train prosecutors on investigating national security cyber crimes, and to coordinate and de-conflict national security cyber investigations.

Within NSD, the Counter Espionage Section (CES) -- one of NSD's principal litigating components -- is responsible for coordinating and conducting investigations and prosecutions of a wide variety of national security offenses, including economic espionage. CES is home to the Division's experts on the investigation and prosecution of nation state-sponsored and -affiliated cyber actors, including those who engage in the theft of intellectual property.

Interagency Coordination

In addition to investigating and prosecuting Intellectual Property crime, the Department has worked closely with other federal agencies directly, and through the National IP Rights Coordination Center ("IPR Center"), to improve IP enforcement domestically and overseas.[5] These activities have included training investigators and prosecutors in the investigation and prosecution of IP crimes; contributing to the Office of the United States 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 United States 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

[5] These federal agencies include Customs and Border Protection ("CBP"), the Federal Bureau of Investigation ("FBI"), the United States Postal Inspection Service ("USPIS"), the Food and Drug Administration's Office of Criminal Investigations ("FDA"), the Department of Commerce's office of Intellectual Property Rights ("DOC"), the Naval Criminal Investigative Service ("NCIS"), the Defense Criminal Investigative Service ("DCIS"), the Defense Logistics Agency ("DLA"), Immigration and Customs Enforcement's Homeland Security Investigations ("ICE"), the United States Nuclear Regulatory Commission ("NRC"), the United States Patent and Trademark Office ("USPTO"), the General Service Administration's Office of Inspector General ("GSA"), the Consumer Product Safety Commission ("CPSC"), the National Aeronautics and Space Administration ("NASA"), the Department of State's Office of International Intellectual Property Enforcement ("IPE"), the Army Criminal Investigation Command's Major Procurement Fraud Unit ("MPFU"), and the Air Force Office of Special Investigations ("AFOSI").

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 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.

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

- **Criminal Enforcement / Policy Working Group:** This working group assesses the Department's IP enforcement efforts, policies, and strategies, and makes recommendations where appropriate, including evaluating the need for legislative changes to key federal statutes and the United States Sentencing Guidelines to address gaps or inadequacies in existing law, changing technology, and increasingly sophisticated methods of committing IP offenses.

- **Domestic and International Outreach and Education Working Group:** This 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:** This working group identifies opportunities for increased civil IP enforcement and legislative action on civil law.

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, among other things:

- 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 Section (a)(7)(B) below.

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

As part of the IP Task Force initiative, the Department achieved notable success in FY 2013 both domestically and abroad. Some of these efforts are highlighted below:

Prosecution Initiatives

Through its IP Task Force, the Department identified three enforcement priorities for IP investigations and prosecutions, including offenses that involve (1) health and safety, (2) trade secret theft or economic espionage, and (3) large-scale commercial counterfeiting and piracy. The Department has also increased its focus on IP crimes that are committed or facilitated by use of the Internet or perpetrated by organized criminal networks.

(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, automotive parts, and military goods. In FY 2013, this initiative resulted in a number of significant prosecutions, including those set forth below:

- *North Carolina Man Pleads Guilty to Trafficking in Counterfeit Airbags*. On September 30, 2013, Igor Borodin, 27, of Indian Trail, North Carolina, was sentenced to 84 months in prison, and ordered to forfeit his residence, after pleading guilty to trafficking in counterfeit airbags he purchased from China and resold through eBay. Borodin sold an estimated 7,000 counterfeit airbags online, and earned at least $1.7 million in revenue. (WDNC, ICE, DOT-OIG)

- *California Woman Sentenced for Trafficking in Counterfeit Cosmetics.* On September 23, 2013, Crystal Dawn Gray, 32, of Orosi, California, was sentenced to nine months home confinement and five years probation after pleading guilty to trafficking in counterfeit cosmetics. Gray was also ordered to pay more than $30,000 in restitution. Gray purchased counterfeit cosmetics and accessories from an Internet retailer outside of the United States and resold them as genuine MAC brand items. (EDCA, ICE)

- *Washington Man Sentenced for Trafficking in Counterfeit Vehicle Airbags.* On September 20, 2013, Vitality Yaremkiv, of Vancouver, Washington, was sentenced to six months in prison for trafficking in counterfeit airbags. Between June 2011 and June 2012, Yaremkiv sold more than 900 counterfeit Honda, Subaru, and Toyota airbags that he imported from a source in China generating $137,243 in sales. (WDWA, FBI, ICE)

- *Two Men Charged in Texas and Arrested for Smuggling Counterfeit Viagra.* On August 6, 2013, Jamal Khattab, 49, of Katy, Texas, and Fayez Al-Jabri, 45, of Chicago, were arrested for conspiring to traffic in counterfeit and misbranded medicine. According to the indictment, the defendants smuggled counterfeit Viagra from China into the United

States and delivered approximately 17,000 counterfeit and misbranded Viagra tablets to an undercover agent. (CCIPS, SDTX, ICE, FDA, DSS)

- *Missouri Firm Pleads Guilty to Importing Products with Counterfeit Safety Labels.* On July 15, 2013, a Springfield, Missouri company, GuildMaster, Inc., pleaded guilty to importing thousands of lamps from its manufacturer in China bearing counterfeit safety certification labels. As part of its plea, GuildMaster acknowledged that, had it inspected the lamps, it would have seen counterfeit and unauthorized Underwriters Laboratory ("UL") marks. Under the terms of the plea agreement, GuildMaster will forfeit thousands of lamps valued at approximately $1,830,000 and will be placed on a five-year term of probation. (WDMO, ICE)

- *Automotive Parts Suppliers Plead Guilty to Selling Counterfeit Replacement Parts.* On July 2, 2013, Fadi Kilani, 28, of Englewood, New Jersey, pleaded guilty to conspiracy to traffic in counterfeit goods and trafficking in counterfeit goods. On June 18, 2013, Shashi Malhotra, 67, of Norwood, New Jersey, pleaded guilty for his role in the same conspiracy. Malhotra and Kilani repackaged and sold aftermarket automotive parts – including brakes, anti-lock braking sensors, ignition coils, and water pumps – which did not meet independent federal safety standards. The defendants sold these auto parts as being manufactured by Ford Motor Company, General Motors ("GM"), and Federal Mogul. (SDNY, FBI)

- *Thousands of Domain Names Associated With the Sale of Counterfeit Pharmaceuticals Seized as Part of "Operation Pangea."* In FY 2013, as in prior years, the Department assisted in the seizure of thousands of domain names as part of Operation Pangea, an annual week-long global enforcement effort aimed at disrupting the organized crime networks behind the illicit online sale of fake drugs. Notable FY 2013 seizures under Operation Pangea include the following:

    - On June 27, 2013, as part of Operation Pangea VI, the Department seized more than 1,600 domain names associated with websites selling counterfeit or misbranded drugs, including Avandaryl, Celebrex, Levitra, Viagra, and Clozapine. As a result of the global operation, more than 10 million illicit and counterfeit pills worth more than $35 million were confiscated, 13,700 websites were shut down, and 213 individuals were placed under arrest or under investigation. (DCO, FDA, INTERPOL)
    - On October 3, 2012, as part of Operation Pangea V, the Department assisted in the seizure of 686 domain names associated with websites unlawfully distributing counterfeit pharmaceuticals. As a result of the global operation, more than 3.5 million illicit and counterfeit pills worth more than $10 million were confiscated, 18,000 websites were shut down, and 80 individuals were placed under arrest or under investigation. (CCIPS, DMD, ICE, CBP, FBI, FDA)

- *Man Charged with Selling Counterfeit Semiconductors for Use on Nuclear Submarines*. On June 25, 2013, Peter Picone, 40, of Methuen, Massachusetts, was charged with importing counterfeit semiconductors into the United States. According to the

indictment, Picone purchased counterfeit semiconductors from sources in Hong Kong and China, made false representations about their authenticity, and sold them throughout the United States, including to companies he believed to be defense contractors. Certain semiconductors sold by Picone were intended for use on nuclear submarines. Trial is scheduled for 2014. (CCIPS, DCT, DCIS, ICE, NCIS)

- *Florida Man Sentenced for Counterfeit Razor Blades.* On June 17, 2013, Jeffrey Steven Telsey, 56, of Delray Beach, Florida, was sentenced to 30 months in prison and ordered to pay more than $400,000 in restitution for conspiring to traffic in counterfeit Gillette razorblades. As part of the investigation, Agents seized approximately 27,000 units of counterfeit Gillette-branded razors from the Defendant's business, valued at approximately $425,000. (WDMI, ICE)

- *Defendants Sentenced for Trafficking in Counterfeit Toys Containing Lead.* On May 30, 2013, Hung Lam, 55, and Isabella Kit Yeung, 37, both of Miami-Dade County, Florida, were sentenced to 22 months in prison and one year of probation, respectively, for their roles in smuggling hazardous children's products from China. In addition, defendants were ordered to forfeit $862,500 and other property. From approximately April 2000 through May 2011, defendants conspired to sell children's products imported from China, including toys that contained banned hazardous substances such as lead and small parts that presented the risk of choking, aspiration, and ingestion. (SDFL, ICE, CPSC, CBP)

- *Group Charged for Importing and Selling Hazardous and Counterfeit Toys.* On February 6, 2013, a 24-count indictment was unsealed in Brooklyn, New York, charging five individuals and corporations with trafficking in hazardous and counterfeit toys. According to the indictment, from July 2005 through January 2013, the individual defendants used their companies to import hazardous and counterfeit toys from China bearing copyright-infringing images and counterfeit trademarks that they sold, both wholesale and retail. The toys were found to contain excessive lead and phthalate levels, small parts that presented choking, aspiration, or ingestion hazards, and easily accessible battery compartments. (CCIPS, EDNY, ICE, NYPD, CPB, CPSC)

- *Saxe Man Sentenced for Trafficking in Counterfeit GM Diagnostic Equipment.* On January 11, 2013, Justin DeMatteo, 31, of Saxe, Virginia, was sentenced to serve one year in prison, and to forfeit more than $430,000, for selling counterfeit GM automotive diagnostic devices used by mechanics to identify problems with, and assure the safety of, motor vehicles. This case was part of "Operation Engine Newity," an international initiative targeting the production and distribution of counterfeit automotive products that impact the safety of the consumer. (CCIPS, EDVA, FBI, IPR Center)

- *Orange County Man Sentenced for Trafficking in Counterfeit Exercise Equipment.* On December 10, 2012, Stanley Kuo Jua Yang, 36, was sentenced to 30 months in prison for trafficking in counterfeit goods, including counterfeit exercise equipment purporting to be Malibu Pilates, Bowflex, and Ab Circle Pro. As part of the investigation, federal agents seized approximately $900,000 worth of counterfeit goods from the defendant. (CDCA, ICE, CBP)

- *Alleged Trafficker of Counterfeit Automotive Accessories Indicted in Virginia.* On October 25, 2012, Katiran Lee, 39, an Indonesian national, was indicted for allegedly participating in a conspiracy to sell to United States consumers more than $3 million worth of counterfeit GM and BMW automotive diagnostic devices and other automotive equipment. Such diagnostic devices are used by mechanics to identify problems with, and assure the safety of, motor vehicles employing electronic control systems. (CCIPS, EDVA, FBI)

- *New Zealand Doctor Sentenced to 18 Months for Trafficking in Counterfeit Drugs.* On October 11, 2012, Robin Han, 43, a physician and citizen of New Zealand, was sentenced to serve 18 months in prison and pay over $196,000 in restitution after pleading guilty to three counts of criminal counterfeiting. According to the indictment, Han advertised the sale of counterfeit pharmaceuticals on a number of websites, including alibaba.com. The parcels Han shipped contained packing slips which falsely claimed the contents were plastic stationery holders and pen boxes. (CDCA, ICE, CBP)

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

In FY 2013, consistent with the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets and the IP Task Force's priorities, Department prosecutors and the FBI have continued to emphasize the investigation and prosecution of commercial and state-sponsored trade secret theft. This continuing focus has led to the investigation and prosecution of numerous trade secret cases and economic espionage cases. Recent cases include:

- *Sinovel Corporation and Three Individuals Charged with Theft of AMSC Trade Secrets*. On June 27, 2013, Sinovel Wind Group, a China-based manufacturer and exporter of wind turbines, two Sinovel employees, and another individual were indicted for their role in stealing trade secrets from AMSC (formerly known as American Superconductor, Inc.), a United States corporation. Sinovel is charged with recruiting an AMSC employee to join Sinovel and to secretly copy copyrighted and trade secret information from AMSC's computer system. Sinovel obtained this information to produce wind turbines and to retrofit existing wind turbines with AMSC's technology without having to pay AMSC for the use of its technology. Sinovel further used the theft to avoid paying AMSC for more than $800 million in products and services that AMSC had already provided to Sinovel, but for which Sinovel had not yet paid. (CCIPS, WDWI, FBI)

- *Two Sentenced in Conspiracy to Steal GM Trade Secrets.* On May 9, 2013, Shanshan Du, 51, and her husband, Yu Qin, 49, of Troy, Michigan, a former GM engineer, were sentenced to one year and three years in prison, respectively, for conspiring to steal and use hybrid technology trade secrets from GM. The defendants copied more than 16,000 GM files to an external computer hard drive, and they later used the information in a business venture to provide hybrid vehicle technology to a China-based automotive manufacturer and competitor of GM. GM estimated the value of the stolen documents at more than $40 million. (EDMI, FBI)

- *Executive Recruiter Convicted of Computer Intrusion and Trade Secret Charges.* On April 24, 2013, a jury convicted David Nosal, 55, of Danville, California, a former employee of Korn/Ferry International, an executive search firm, for conspiring with current and former Korn/Ferry employees to gain unauthorized access to Korn/Ferry's computer system and steal trade secrets to use in a new business that Nosal intended to establish with them. Two of those employees downloaded large numbers of "source lists" prior to their own departures from Korn/Ferry. Thereafter, those employees used the Korn/Ferry log-in credentials of another conspirator still employed at Korn/Ferry to download additional information from Korn/Ferry's computer system. Sentencing is scheduled for December 18, 2013. (CCIPS, NDCA, FBI)

- *Defense Contractor Sentenced to 70 Months for Exporting Military Technology to China.* On March 25, 2013, Sixing Liu, a/k/a, "Steve Liu," 49, a Chinese national and former New Jersey-based defense contractor employee, was sentenced to 70 months in prison after he was convicted by a jury of exporting sensitive United States military technology to China, stealing trade secrets, and lying to federal agents. Liu stole thousands of electronic files from his employer, L-3 Communications, containing valuable trade secret information, including files that detailed the performance and design of guidance systems for missiles, rockets, target locators, and unmanned aerial vehicles. Liu stole the files to position and prepare himself for future employment in China. As part of that plan, Liu delivered presentations about the technology at several Chinese universities, the Chinese Academy of Sciences, and conferences organized by Chinese government entities. (DNJ, ICE, CBP)

- *Former Silicon Valley Engineer Sentenced to Prison For Stealing Marvell Trade Secrets.* On February 25, 2013, Suibin Zhang 44, of Belmont, California, was sentenced to three months in prison, three years of supervised release, 200 hours of community service and ordered to pay $75,000 in restitution to the victim, Marvell Semiconductor, Inc. ("Marvell"), following his conviction on five counts of trade secret theft. While employed as a project engineer at Netgear Inc., Zhang had access to the secure database of Marvell. After accepting a position with a competitor, Zhang used his Netgear account to download Marvell trade secrets and proprietary information and then loaded the trade secrets onto a laptop for his new employer. (NDCA, FBI)

- *Texas Man Sent to Prison for Attempted Theft of Trade Secrets.* On February 8, 2013, Steven Thomas Stancil, 52, of Magnolia, Texas, was sentenced to 10 months (five months in prison and five months home confinement), three years of supervised release, and 200 hours of community service for attempted theft of trade secrets. Stancil, who worked as a cost analyst for Mogas Industries Inc., downloaded proprietary company information from his company computer and sent emails to approximately eight Mogas competitors offering to sell the proprietary information, including all drawings and designs, customer contacts, vendors, pricing, and more. Stancil also emailed at least one Mogas competitor numerous files containing proprietary images of schematic drawings and measurements of valve parts manufactured by Mogas. (SDTX, FBI)

- *Kentucky Men Charged with Attempting to Steal Trade Secrets from Their Former Employer.* On October 9, 2012, Phillip Lee Groves, Gregory Lee Wampler, and Eric Dale Tinderholt, all of Christian County, Kentucky, were indicted for conspiring to steal trade secret information from Groves and Wampler's former employer, White Drive Products, Inc. Groves downloaded 125 files containing trade secret information that he and Wampler used as leverage to obtain employment at a competitor. Tinderholt is charged with knowingly receiving and possessing stolen trade secret information. (WDKY, FBI)

- *Kolon Industry Executives Indicted for Stealing DuPont Trade Secrets.* In March 2013, a superseding indictment was brought against Kolon Industries, Inc., a South Korean-based corporation, and five of Kolon's top executives for conspiracy to convert trade secrets, theft of trade secrets, and obstruction of justice. These charges superseded an indictment made public in October, 2012. Kolon is accused of recruiting former and current DuPont employees over a period of several years in order to obtain trade secret information regarding the manufacture of high-strength para-aramid fibers, commonly known as "Kevlar." The indictments also seek forfeiture of at least $225 million dollars from Kolon. In a parallel civil proceeding, DuPont won a $920 million verdict against Kolon in September 2011. (EDVA, FBI)

- *U.S. and Chinese Defendants Charged with Conspiring to Sell Trade Secrets to Chinese Companies.* In February 2012, a San Francisco grand jury indicted five individuals and five companies with conspiring to commit economic espionage and trade secret theft, among other offenses, in connection with the theft of pigment technology from E .I. du Pont de Nemours & Company (DuPont). This was the first indictment of a Chinese state-owned enterprise by a U.S. grand jury. Trial in the matter is scheduled for January 2014. (NDCA, CES, FBI)

(3) Large-Scale Commercial Counterfeiting and Online Piracy

The Department continues to pursue significant, large-scale piracy and counterfeiting operations. In FY 2013, the Department has had a number of si*g*nificant prosecutions, including those set forth below:

- *Texas Residents Sentenced in Counterfeit DVD/CD Ring.* On July 23 and August 9, 2013, Ruth Gloria Henneberger, 36, Joe Silvas, 43, Daniel Diaz, 34, William Joseph Henneberger, 32, and Leticia Perez Aguilar, 39, were each sentenced for criminal copyright infringement. All defendants participated in the reproduction and distribution of thousands of pirated DVDs and music CDs causing close to $750,000 dollars in losses to victim companies. (SDTX, ICE, CBP)

- *Chinese Man Sentenced to 12 Years for Theft of Over $100 Million in Proprietary Data.* On June 11, 2013, Xiang Li, 36, of Chengdu, China, was sentenced to 12 years in prison for conspiracy to commit wire fraud and criminal copyright infringement for selling $100 million worth of pirated, sensitive, industrial-grade software to over 400 customers located in at least 28 states and over 60 foreign countries and selling 20 gigabytes of confidential and

proprietary data stolen from the internal server of a defense contractor. Li's customers included those in embargoed countries in the Middle East, foreign government employees, and federal government employees and contractors holding security clearances. The software included applications intended for use in radio transmissions, radar, microwave technology, and vacuum tubes used in military helicopters. (DDE, ICE, DCIS)

- *Baltimore Man Sentenced to Over 7 Years for Pirating Commercial Software Programs.* On June 6, 2013, Naveed Sheikh, of Baltimore, Maryland, was sentenced to 87 months in prison for conspiracy to reproduce and distribute more than 1,000 infringing copies of copyrighted commercial software programs worth over $4 million. The software included Microsoft Office, Windows XP, Adobe Acrobat, Photoshop, and Quicken Premier Home. Sheikh was also ordered to pay $4 million in restitution to the victims. (DMD, FBI, ICE, USPIS)

- *Two Convicted of Counterfeiting Thousands of Luxury Goods.* On April 24, 2013, Yintang Cao, 48, and Hong Zhang, 46, both Chinese nationals, pleaded guilty to trafficking more than 14,000 counterfeit luxury goods bearing the names of Coach, Dolce & Gabbana, Louis Vuitton, Prada, and Versace. Sentencing is scheduled for December 13, 2013. (SDTX, ICE)

- *Internet Piracy Group Member Sentenced to 23 Months for Criminal Copyright Conspiracy.* On April 10, 2013, Javier E. Ferrer, 41, of New Port Richey, Florida, was sentenced to 23 months in prison for his role in IMAGiNE, an organized online piracy ring that was the premier motion picture pre-release group during its operation. Ferrer and his co-conspirators illegally obtained and disseminated digital copies of copyrighted motion pictures only showing in theaters. The leader of the group, Jeramiah B. Perkins, was previously sentenced to 60 months and co-defendants Sean M. Lovelady, Willie O. Lambert, and Gregory A. Cherwonik were, respectively, sentenced to 30 months, 23 months, and 40 months in prison. (CCIPS, EDVA, ICE)

- *Leaders of Counterfeit Goods Ring Sentenced.* On March 28, 2013, Azmi Azzam Al-Hamouri, age 40, and Mahmoud T. Al-Mahmoud, age 34, both of Columbus, Ohio, were sentenced to 15 months in prison and five years probation, respectively, and agreed to pay $1 million in restitution to trademark holders for conspiring to traffic in counterfeit apparel. As part of the investigation, Agents seized four tractor-trailer loads of counterfeit athletic shoes, jeans, watches, and other apparel. (DSC, FBI, Spartanburg Department of Public Safety)

- *Delaware Woman Sentenced to 58 Months for Copyright Infringement and Identity Theft.* On January 24, 2013, Jamie Lynn Snyder, age 35, of Newark, Delaware, was sentenced to 58 months in prison, and ordered to pay a total more than $1 million in restitution for criminal copyright infringement and identity theft. Snyder sold over 24,000 copies of pirated software worth more than $5.9 million. Snyder advertised approximately 400 different software titles on her websites and earned approximately $25,000 to $35,000 per month over a two-year period from her illegal sales. At least 81 different software manufacturers owned the infringed software, including Adobe, Apple, Autodesk, and Microsoft. (DDE, FBI)

- *Washington Company, Owner And Executives Indicted for Trafficking in Counterfeit Goods.* On January 17, 2013, CONNECTZONE.COM LLC, a Lynnwood, Washington electronics company, along with its owner and two employees, were indicted along with Chinese company Shenzhen Xiewei Electronic, LTD, headquartered in Shanghai, China, for conspiracy to traffic in counterfeit goods. The defendants are charged with advertising and selling infringing counterfeit Cisco computer networking products. (WDWA, BEST)

- *Twenty-Two Members of International Counterfeiting Conspiracy Convicted.* On December 14, 2012, LaKeith Fowler, 32, of DeSoto, Texas, was sentenced to 33 months in prison for his role in a large-scale international counterfeiting ring. The defendant was one of 23 individuals charged in the case. Twenty-two of the defendants were convicted, and one defendant was acquitted after a trial in October of 2012. During the course of this international investigation, law enforcement seized over $1 million, over 310,000 pairs of counterfeit Nike sneakers, and a variety of other products and property. The prosecution shut down a large, multi-faceted counterfeiting operation where the sneakers were illegally manufactured in China, transported via container to New York City, and then distributed throughout the United States. (WDNY, ICE)

- *Modesto Woman Sentenced for Counterfeit Music and Movie Conspiracy.* On December 10, 2012, Vicenta Munoz-Peralta, 39, of Modesto, California was sentenced to 46 months in prison for conspiracy to commit criminal copyright infringement and traffic in counterfeit labels, documentation, and packaging. Munoz-Peralta and her co-conspirators manufactured copyright-infringing DVDs worth more than $2 million in a co-defendant's residence in Modesto, which was found to contain approximately 50 printers and several thousand counterfeit CDs and DVDs. Co-conspirator, Jose Alfredo Colorado Munoz, 29, of San Jose, was sentenced to four years in prison on November 19, 2012, and co-conspirator Mariano Vega Hernandez, 25, of Modesto was sentenced to 46 months on October 15, 2012. (EDCA, FBI, Sacramento Valley Hi-Tech Crimes Task Force)

- *Department of Justice Seizes Hundreds of Domain Names and Millions in Proceeds from Counterfeit Goods as Part of "Operation In Our Sites."* In June 2010, ICE launched "Operation In Our Sites" ("Operation IOS"), which targets online commercial intellectual property crime, including websites offering pirated movies and television shows, as well as a diverse array of counterfeit goods. To date, more than 2,250 domain names of websites engaged in the sale and distribution of counterfeit goods and illegal copyrighted works have been seized as a result of Operation IOS. Notable FY 2013 seizures under Operation IOS include the following:

    - On June 26, 2013, as part of Projects American Icon and Project Transatlantic Two, United States authorities announced the seizure of 328 domain names associated with websites selling counterfeit goods bearing trademarks of American-owned companies, including Rosetta Stone, NFL, BEATS by Dre, Tiffany & Co, Nike, Ergo, MLB, NBA, and NHL. Agents also seized illegal proceeds in excess of $150,000 from PayPal accounts. (CCIPS, DCO, DNJ, WDTX, EDLA, ICE, IPR Center, Europol)

- On November 26, 2012, as part of Project Cyber Monday 3 and Project Transatlantic, the Department assisted in the seizure of 132 domain names used to sell counterfeit merchandise online to unsuspecting consumers. Visitors typing those domain names into their Web browsers will now find a banner that notifies them of the seizure and educates them about the federal crime of willful copyright infringement. (CCIPS, DMD, DCOLO, SDCA, CDCA, WDNY, WDTX, ICE, IPR Center)

- *Annandale Man Sentenced to 36 Months for $2.5 Million Software Piracy.* On November 9, 2012, Quynh Trong Nguyen, 36, of Annandale, Virginia was sentenced to 36 months in prison for selling counterfeit and altered computer software. Nguyen was also ordered to pay $2.5 million in restitution and to forfeit $1.4 million. Over a three and a half year period, Nguyen sold more than $2.5 million in copyright-infringing computer software and defrauded more than two thousand customers. Much of the software was shipped from overseas and included popular titles such as Adobe Acrobat, Microsoft Office, and Autodesk AutoCAD. (EDVA, ICE, USPIS)

- *Michigan Man Charged with Selling Counterfeit Software Worth More Than $1.2 Million.* On November 8, 2012, Bruce Alan Edward, 48, of Atlanta, Michigan, was arraigned on charges of mail fraud and selling more than 2,500 copies of counterfeit Microsoft software worth more than $1.2 million. Edward unlawfully distributed counterfeit copies of Microsoft Office 2003 Professional and Windows XP Professional by purchasing counterfeit copies from China and Singapore and selling the works on eBay. (CCIPS, EDMI, ICE)

- *California Man Sentenced to Year for Trafficking in More Than 30,000 Counterfeit DVDs.* On October 22, 2012, Jackie Weisheng Chen, 48, of Arcadia, California, was sentenced to one year in prison for trafficking in more than 30,000 DVDs with counterfeit trademarks of Dolby Laboratory Licensing Corporation. Chen, the owner of Temia Media, continued to sell the counterfeit DVDs despite multiple notices from CBP and three prior seizures of more than 5,000 DVDs with counterfeit Dolby trademarks. (CDCA, CBP, ICE)

- *Seven Michigan Individuals Sentenced for International Counterfeit Goods Conspiracy.* On October 16, 2012, Hassan Aoun, 43, of Dearborn, Michigan, was sentenced to 36 months in prison after being convicted by a jury for conspiracy to traffic in counterfeit goods and trafficking in counterfeit goods. Between 2004 and 2010, the Aoun Organization imported counterfeit goods that they sold as luxury name brand products, including Nike, Gucci, and Timberland shoes; Coach, Christian Dior and Louis Vuitton purses; and clothing lines from brands such as Diesel Jeans, Burberry, Lacoste, Coogi, and professional sports teams. In addition to Hassan Aoun, six other members of the Aoun Organization have been sentenced for their participation in the conspiracy. (EDMI, FBI, IRS)

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 FY 2013, the Criminal Division coordinated with the IPR Center's IP Theft Enforcement Team to provide training to ICE agents, CBP officers, and state and local law enforcement agents in Houston, Texas (December 2012) and Tucson, Arizona (March 2013).

- In November 2012, NSD, with support from CCIPS, organized and led the first NSCS Network training conference in the Washington, D.C. area. The NSCS Network is a nationwide network of prosecutors and other attorneys, whose members are specially trained to investigate computer crimes that have a national security dimension, including the theft of IP and other information by nation state actors. Many members of the NSCS Network are also members of the CHIP Network where appropriate. The NSCS training builds on the technical skills covered by the CHIP conference to address the added complexity of working with classified information and related issues to investigate, prosecute, and otherwise disrupt those crimes. A second training conference was held in November 2013.

- In January 2013, CCIPS organized and taught the Computer Forensics Seminar at the NAC in Columbia, South Carolina. This seminar, which was attended by more than 40 prosecutors and federal agents, used case scenarios involving IP crime to provide a number of strategies and techniques for identifying and analyzing electronic evidence, and for admitting electronic evidence in court.

- In March 2013, CCIPS organized the Trade Secret and Economic Espionage Seminar at the NAC in Columbia, South Carolina. This seminar, which was attended by approximately 50 prosecutors and federal agents, provided substantive instruction on investigating and prosecuting trade secret theft through case studies, as well as in-depth guidance on discovery issues, parallel proceedings, working with industry, sentencing, and valuation.

- From April 22 through April 25, 2013, CCIPS prosecutors trained over 100 members of the national CHIP coordinators' network at the NAC in Columbia, South Carolina. The annual training, which brought together CHIP prosecutors from United States Attorneys' Offices across the United States, as well as several Department components, examined recent IP prosecutions, as well as techniques for investigating and trying IP crimes.

- In June 2013, CCIPS prosecutors trained approximately 30 FBI and ICE agents in Washington, D.C. on the investigation and prosecution of IP crimes, the statutory framework of United States criminal IP statutes, and building prosecutable copyright, trademark, and Economic Espionage Act cases.

- In August 2013, CCIPS prosecutors provided training to over 30 agents, analysts, and supervisors from 23 FBI divisions. The training, which was held at the FBI Academy in Quantico, Virginia, included an overview of U.S. IP law and also surveyed legal perspectives and requirements for criminal IP prosecutions.

- In September 2013, CCIPS organized and taught the Electronic Evidence and Basic Cybercrime Seminar at the NAC in Columbia, South Carolina. This seminar, which was attended by more than 60 prosecutors and federal agents, provided instruction on the Electronic Communications Privacy Act, the Internet for prosecutors, surveillance techniques, international issues, IP crimes, and other topics.

- The Bureau of Justice Assistance 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 FY 2013 in locations such as Burbank, California; Bismarck, North Dakota; Philadelphia, PA; and Cape Elizabeth, Maine.. The goal of the seminars was to increase the quantity and quality of investigations and prosecutions of IP crime by state and local law enforcement. For a full list of training locations, please see section (a)(1) of this report.

International Outreach and Training

Global IP crime, from the manufacture and worldwide distribution of counterfeit goods, to the sprawling online businesses designed to reap profits from the distribution of copyrighted works, continues to grow and change in an effort to stay ahead of law enforcement authorities. As a world leader in efforts to combat criminal IP infringement, the Department actively seeks to develop training and technical assistance programs to assist other countries in effectively enforcing IP laws and reducing the trafficking of counterfeit and pirated goods. Despite budgetary constraints, in FY 2013 the Department worked extensively with its law enforcement counterparts around the world. The Department sought to engage foreign law enforcement through meetings of officials, ranging from the Attorney General to line attorneys and agents.

CCIPS and DOJ's Office of Overseas Prosecutorial Development, Assistance and Training ("OPDAT") worked with State Department grants and in cooperation with other United States agencies in FY 2013 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 awareness amongst enforcement officials and the judiciary of the importance of reducing counterfeiting and piracy. FY 2013 saw the placement of an experienced CHIP attorney as the third IP Law Enforcement Coordinator ("IPLEC") in Bangkok, and the agreement by the State Department to fund the placement of an IPLEC in Eastern Europe (a role that has been vacant since 2011). Additionally, DOJ continued to engage with China through the bilateral IP Criminal Experts Working Group ("IPCEWG") of the Joint Liaison Group ("JLG") and continued multi-year projects to improve law enforcement capacity to protect IP. The following discussion summarizes those efforts.

CHINA

Annual Meeting of US-China Joint Liaison Group on Law Enforcement Cooperation. In December 2012, CCIPS attorneys traveled to Guangzhou, China, to participate in the 10th Annual Meeting of the Joint Liaison Group on Law Enforcement Cooperation ("JLG"). The

JLG is designed to strengthen law enforcement cooperation between the United States and China across a range of issues, including intellectual property and cyber crime. As co-chair, CCIPS' Deputy Chief led the IPCEWG meeting, including a discussion of the identification of new initiatives for cooperation. Also in attendance at the JLG meeting were additional representatives from DOJ, DOS, FBI, and ICE. Although an interim IPCEWG meeting was scheduled to take place in October 2013 in China, the Department was unable to attend due to the government shutdown.

Meetings with Chinese Law Enforcement Delegation. In January 2013, CCIPS participated in a series of meetings with a Chinese law enforcement delegation in New York, New York; Newark, New Jersey; and Crystal City, Virginia. These meetings included discussions regarding ongoing and new initiatives for cooperation between United States and Chinese law enforcement on IP enforcement. The eight-person Chinese delegation included officials from the Ministry of Public Security, the Guangdong Provincial Public Security Department, and the Guangzhou Municipal Public Security Bureau.

AFRICA

African IP Protection Summit. In March 2013, CCIPS facilitated and co-organized with the Department of Commerce a workshop on the "Practical Approaches to IP Utilization and Protection in Africa," in Dar Es Salaam, Tanzania. Almost three years in the making, this first-of-its-kind event brought together international private sector leaders, government officials, and IP stakeholders from across Africa to discuss practical approaches, successes, challenges, and future strategies to increase the protection and utilization of IP as a facilitator of innovation, entrepreneurship, trade, and investment. Participants included about 150 East, West, and Southern African IP officials and private sector representatives, including prosecutors, judges, investigators, customs officials, and IP registration offices.

Southern African IP and Financial Crime Training. In late February and early March 2013, CCIPS and OPDAT travelled to Cape Town, South Africa to organize the "Pilot Course on Financial Investigative Skills for Intellectual Property and Other White Collar Crimes." Other members of the United States delegation include FBI Legal Attaches, AUSAs, and IRS Special Agents. Fifty law enforcement representatives from South Africa, Botswana, Nigeria, and Tanzania attended. Designed by the DOJ and IRS, this innovative training addressed how financial investigations can support the prosecution of IP cases.

Criminal Enforcement Assessment in Namibia. In late January and early February 2013, CCIPS and OPDAT, with the collaboration of INTERPOL, traveled to Windhoek, Namibia, for an IP criminal enforcement assessment mission. During the assessment, DOJ attorneys met with various Namibian government officials, including prosecutors, regulatory bodies, IP offices, customs, tax authorities, money laundering officials, and judges, as well as with INTERPOL officials and the United States Ambassador to Namibia.

IP Training at ILEA in Botswana. In January 2013, CCIPS travelled to Gaborone, Botswana, to participate in the "2013 ILEA Botswana Intellectual Property Theft Enforcement Training"

organized by DHS and to present on several IP related topics. Attendees included 50 law enforcement officials from Botswana, Ghana, Mauritius, Nigeria, Seychelles, and Swaziland.

African Anti-Counterfeiting Training with INTERPOL. In October 2012, CCIPS, OPDAT, and INTERPOL organized a conference entitled, "Integrated Criminal Enforcement Training against Trafficking in Illicit Goods" in Dar Es Salaam, Tanzania. The three-day training covered methodology used in identifying, targeting, and dismantling transnational organized crime groups involved in the manufacture and distribution of counterfeit goods. In attendance were more than 50 officials from police, prosecutor's offices, customs, intellectual property agencies, as well as intellectual property law enforcement experts from Tanzania and from neighboring countries, including Burundi, Uganda, Kenya, Rwanda, and Congo.

MEXICO

Online Copyright Training for Judges. In September 2013, CCIPS facilitated training on "Copyright Enforcement in the Digital Environment" for 20 Mexican judges in Mexico City, Mexico. CCIPS took part in, and moderated, various panel discussions focused on prosecution of copyright crimes.

Presentation to Mexican Officials on Prosecuting Online Copyright Crimes. In August 2013, CCIPS presented at a seminar in Mexico City entitled, "Copyright in the Digital Environment." The seminar, sponsored by the United States Embassy in Mexico and the USPTO's Attaché to Mexico City, featured several roundtables focused on the enforcement of copyright laws. The audience included more than 50 Mexican government officials and leading private attorneys.

IP Accreditation of Mexican Advisors. In June 2013, with the cooperation of OPDAT and the World Customs Organization ("WCO"), CCIPS traveled to Brussels, Belgium, to support the competitive testing by WCO of three Mexican Intellectual Property Technical Operational Advisors. These officials were identified and prepared by DOJ over several years for this event. Based on their success in the accreditation process, the advisors will serve as WCO world accredited experts in customs and IP, as liaison with prosecutors, and as worldwide customs trainers. This is the third group of Mexican officials that DOJ has supported in seeking accreditation.

Assisting in IP Enforcement in Mexico. In April 2013, with the assistance of OPDAT, CCIPS conducted assessment meetings with representatives of Mexican agencies that handle issues related to enforcement of IP crimes in Mexico City, Mexico. CCIPS met with the Director General of Aduanas (Mexican Customs and Tax), Indautor (Mexican Copyright Office), IMPI (Mexican Patent and Trademark Office), Cofepris (Mexican Food and Drug Administration), and with the heads of different divisions at the Mexican Attorney General's Office, including intellectual property, organized crime, training, financial crimes, and witness protection.

IP Workshops for Mexican Enforcement Agencies. In May 2013, with the assistance of OPDAT and the WCO, CCIPS organized and facilitated workshops on "Interagency Cooperation for Enforcement of Intellectual Property at the Border" in Mexico City, Lazaro-Cardenas, and

Manzanillo. The workshop included 40 officials from Mexican Customs, IMPI (Patent and Trademark Office), Indautor (Copyright Office) and Cofepris (FDA).

Train-the-Trainer Program for Criminal IP Enforcement in Mexico. In February 2013, CCIPS organized the third phase of a Train-the-Trainers Workshop on Criminal IP Enforcement at the Border for Mexican customs officials. This program took place in Costa Rica and was presented with the assistance of OPDAT, the WCO, and law enforcement authorities in San Jose, Costa Rica. Mexican officials (previously prepared by DOJ and WCO) trained law enforcement authorities in Costa Rica on customs issues affecting criminal enforcement of intellectual property.

Mexican Criminal IP Enforcement Training. In December 2012, CCIPS, DOJ's Senior Resident Legal Advisor in Mexico, and OPDAT organized and presented the second part of a Train-the-Trainers' Workshop on Criminal Enforcement at the Border. The Workshop addressed cutting edge teaching techniques, practice in Mexico's new adversarial system, and chain-of-custody issues for Mexican prosecutors and customs officials.

OTHER REGIONS

Third Conference of the IP Crimes Enforcement Network. In May 2013, CCIPS and DOJ's IPLEC for Asia hosted the third IP Crimes Enforcement Network ("IPCEN") Conference in Bangkok, Thailand. Sponsored by CCIPS, OPDAT, and the United States Embassy, the IPCEN Conference is designed to help prosecutors and investigators in the region to develop a network of IP enforcement authorities and foster bilateral and regional cooperation. Sixty IP crime investigators and prosecutors from the 10 members of the Association of South East Asian Nations ("ASEAN"), as well as South Korea and China, attended the two day conference.

IP Enforcement Training Program at ILEA Budapest. In December 2012, the International Law Enforcement Academy ("ILEA") in Budapest hosted a 4-day program on IP enforcement for approximately 40 police, prosecutors, and customs officials from Hungary, Bulgaria, Romania, and the Slovak Republic. CCIPS, along with representatives from FBI, ICE, and CBP, provided instruction on IP laws, law enforcement practices, and information-sharing. Also participating in the program were experienced IP prosecutors and customs officials from several EU member states and representatives of private rights owners and trade groups in Europe.

Computer Forensics Training for Middle East/North African Prosecutors. In February 2013, CCIPS trained approximately 40 prosecutors and investigators at the "Regional Workshop on Investigating and Prosecuting Intellectual Property Violations" in Amman, Jordan. Sponsored by OPDAT and CCIPS, the workshop was designed to help prosecutors and investigators in the region develop a network of IP enforcement authorities and foster bilateral and regional cooperation. The Workshop was attended by prosecutors and investigators from Egypt, Jordan, Lebanon, Morocco, Saudi Arabia, and the United Arab Emirates.

Intellectual Property Training in Lima, Peru. In April 2013, CCIPS participated in and presented at an IP training workshop organized by the IPR Center at the ILEA in Lima, Peru. An

audience of approximately 50 attendees took part, consisting of prosecutors and investigators from Andean Pac countries.

Weeklong IPR Enforcement Training for Bulgaria, Serbia, and Moldova. In May 2013, CCIPS helped organize and teach a weeklong course on intellectual property rights enforcement at the ILEA in Budapest, Hungary, for about 30 prosecutors, police, and customs officers from Bulgaria, Serbia, and Moldova. ICE sponsored the conference.

CCIPS Meets with Delegates of 14 Countries. In FY 2013, as part of the Department's International Visitors Program, the Department met with 92 visitors from more than 14 countries to coordinate on issues related to international IP and cybercrime investigation and prosecution. Visiting delegations included representatives from Sri Lanka, China, Brazil, Peru, Netherlands, Kuwait, France, Kazakhstan, Italy, Burma, India, Belgium, Croatia, and Vietnam.

Outreach to the Private 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' Annual IPR Industry/Law Enforcement meeting in July 2013, in Washington, D.C. The meeting provided representatives from a broad range of 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 remarks by Deputy Attorney General James M. Cole and Acting Assistant Attorney General Mythili Raman. Senior law enforcement officials from the FBI, ICE, CBP, and FDA 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, symposia, and workshops attended by IP rights holders and law enforcement officials. These events included, among others: the Underwriters Laboratory Brand Protection Wire and Cable Summit in Melville, New York, in October 2012; International Anti-Counterfeiting Coalition ("IACC") Foundation's Training Seminar for federal and local law enforcement in San Diego, California, in October 2012; American Intellectual Property Law Association's ("AIPLA") annual conference in Washington, D.C., in October 2012; and the Underwriters Laboratories Brand Protection Workshop in Fort Lauderdale, Florida, in June 2013.

Similarly, NSD's leadership and other attorneys have reached out to senior managers at more than 30 companies over the last year to educate them about the Department's resources and efforts to combat trade secret theft and other national security cyber threats. These outreach efforts have taken the form of presentations at regional conferences, like Assistant Attorney General Lisa Monaco's presentation to the ABA Standing Committee on Law and National Security in January 2013, and one-on-one meetings with senior executives at Fortune 500 and

other companies. The NSCS Network also disseminated talking points and other presentation materials to all members of the Network nationwide to facilitate their outreach to companies in their home districts.

On November 29, 2012, Deputy Attorney General James Cole, Associate Attorney General Tony West, and other high-level Department officials met with the Business Software Alliance. The meeting focused on a range of topics involving IP protection and computer crime.

On February 20, 2013, Attorney General Eric Holder, together with Rebecca Blank, the Acting Secretary of Commerce, provided keynote remarks to launch the Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets. In addition, then Assistant Attorney General Lanny Breuer led a panel of corporate leaders in a discussion of the importance of trade secrets in the modern global economy, as well as the need for businesses to take appropriate actions to safeguard this valuable intellectual property and work cooperatively with law enforcement. A number of United States agencies and affected industries developed and contributed to the strategy, with the Department providing input in the important area of enforcement.

On March 14, 2013, a senior CCIPS official presented at the Hispanic National Bar Association Midyear Corporate Counsel Meeting in Atlanta, Georgia. The presentation, which addressed the Department's IP enforcement efforts and the interaction between industry and law enforcement, was attended by corporate counsel from throughout the country.

On April 2, 2013, a senior CCIPS attorney presented at NYU Law School's Colloquium on Innovation Policy in New York City, New York. The presentation, which was widely attended, addressed the Department's approach to IP enforcement. The Colloquium covered a wide range of issues, including the impact of criminalization on innovation, employee mobility, access to medicines, and developing economies.

On April 9, 2013, a CCIPS representative presented at the White House's annual interagency outreach meeting with the private sector regarding IP Working Groups at United States' embassies around the globe. CCIPS addressed the Department's international IP rights enforcement efforts, and the importance of collaboration between the private sector and the government in uncovering and addressing IP enforcement impediments overseas.

On May 2, 2013, Deputy Attorney General James Cole provided Keynote Remarks at IACC's Spring Conference. The Spring Conference was also attended by a senior CCIPS official who presented on issues surrounding counterfeiting. The conference brought together over 400 brand owners, private investigators, private counsel, and government officials from the United States and abroad to gain a perspective on the trade in counterfeit products, to share best practices on how to effectively combat this illegal trade, and to provide a forum for networking and partnership development.

On May 7, 2013, Deputy Attorney General James Cole led an IP roundtable in Newark, New Jersey, regarding counterfeit and fraudulent medicines, with general counsels and security officers from 15 major pharmaceutical companies. United States Attorney for the District of New Jersey Paul Fishman hosted the event, which was also attended by other representatives

from the Department and various United States Attorney's Offices. The roundtable focused on recent trends and challenges regarding counterfeit and fraudulent medicines and ways the private sector can work with law enforcement to bring counterfeiters to justice.

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 contributes to a National Crime Prevention Council public awareness campaign to help educate the public about IP crime and its consequences, the initial phases of which were introduced November 29, 2011. Since November 2011, the campaign has garnered more than $74.6 million in donated media, including more than 66,337 total airings on television in 209 of 210 nationwide markets and 19,449 airings on radio. In addition, 1,841 digital mall posters have been displayed in 43 nationwide markets; print support for the campaign increased by $30,000 (3.5%) this year; and public service announcements can be seen at 813 elevators in 19 nationwide markets. DOJ and NCPC have also worked with the State Department and US Embassies to get the word out internationally. The campaign was adapted in Bulgaria by PROPHON, a music rights organization, in partnership with the author's society in Bulgaria, the Bulgarian Association of the Music Producers, and the Association of the Radio and TV Broadcasters.

NCPC has traveled to six of the thirteen jurisdictions that received IP theft enforcement grants in 2012 to share the public education campaign and discuss strategies for local law enforcement's use of the campaign products. NCPC is working directly with grantees in Baltimore, Orlando, and Los Angeles to localize announcements from the campaign for use in their communities. The NCPC and the Bureau of Justice Assistance have also completed their data collection efforts to measure attitudinal changes in the public's perception of IP since the unveiling of the campaign. Results indicate the campaign increased awareness, changed behavior, and increased understanding of the term "Intellectual Property" by the American public. Development of new television, outreach tools, and products for use by law enforcement are currently in progress.

(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 provide some insight into 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 2009 - 2013, listing the number of defendants and cases charged, the number of defendants sentenced, and the length of those sentences.[6] 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 cases prosecuted for IP crimes over the course of the last five years. Moreover, as demonstrated by the cases highlighted above, the Department has sought to increase the quality and scope of its investigations and prosecutions over the past years, which is not fully reflected in statistics. Nonetheless, in the last Fiscal Year, the number of IP investigative matters received from law enforcement agencies decreased, and there was a corresponding decrease in the number of IP cases opened and defendants prosecuted.

District Totals	FY2009	FY2010	FY2011	FY2012	FY2013
Investigative Matters Received by AUSAs	285	402	387	390	334
Defendants Charged	235	259	215	254	213
Cases Charged	173	177	168	178	163
Defendants Sentenced	223	207	208	202	205
No Prison Term	126	121	102	95	96

[6] Case statistics were compiled by the Executive office of the United States Attorneys. 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.

1-12 Months	35	38	27	46	35
13-24 Months	29	27	33	26	29
25-36 Months	6	10	17	15	21
37-60 Months	18	7	21	17	19
60 + Months	9	4	8	3	5

(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. Because of resource shortfalls, and the Department's hiring freeze, the actual staffing level is substantially lower. 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.

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 two or more CHIP prosecutors, generally located in the districts that have historically faced the highest concentration of IP and high-tech crimes.

Over the last year, approximately a dozen NSD attorneys have worked on hacking investigations (most of which involve the theft of information, including but not limited to trade secrets). The NSCS Network consists of more than 100 AUSAs and attorneys at Department headquarters who are specially trained in the investigation and prosecution of national security cyber offenses, including the theft of IP and other information.

The IPLEC program currently consists of a Department attorney stationed in Bangkok, Thailand, who has handled IP issues in Asia since January 2006. Between November 2007 and March 2011, a separate Department attorney was stationed in Sofia, Bulgaria, in order to handle IP issues in Eastern Europe. Funding for this position expired in 2011, but the Department has worked with the Department of State to secure alternative funding. Additionally, the President's proposed budget for FY 2014 contains a request to expand and enhance the program by permanently funding up to four Department Attachés who would be cross designated as International Computer Hacking and Intellectual Property ("ICHIP") coordinators. The ICHIP Attachés would be deployed in key locations overseas to assist in implementing the Department's international IP and cybercrime mission.

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 law enforcement 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 brings affirmative cases when United States' intellectual property is infringed, including UDRP proceedings where domain owners have used trademarks owned by the United States in a manner that is likely to confuse the public. 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 duplicate those 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 other agencies. CCIPS also works closely with the CHIP network to assist in coordinating national prosecution initiatives. Along similar lines, NSD and NSCS attorneys closely coordinate with the National Cyber Investigative Joint Task Force, which serves as a focal point for government agencies to coordinate, integrate, and share information related to cyber threat investigations affecting the national security. One NSD attorney works full-time as an onsite liaison between NCIJTF and other members of the NSCS Network. Department attorneys will continue to work with the IPR Center and NCIJTF to identify and de-conflict investigative leads, as well as assist the CHIP and NSCS networks to ensure that investigations and prosecutions are streamlined, not duplicated, and that charges are brought in the appropriate venue.