United States Department of Justice

PRO IP Act
Annual Report FY2014

PRO IP ACT ANNUAL REPORT OF THE ATTORNEY GENERAL FY 2014

INTRODUCTION

The Department of Justice (the "Department") submits this Fiscal Year 2014 ("FY 2014") 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 2014 (*i.e.*, October 1, 2013 through September 30, 2014) are set forth below.

In February 2010, Attorney General Holder 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 has also participated 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 2014, Congress did not appropriate funds for the issuance of state and local law enforcement grants as authorized under Section 401 of the Act.

Nevertheless, in keeping with IP Task Force priorities, the Office of Justice Programs ("OJP") awarded grants to support state and local IP law enforcement task forces and local IP

training and technical assistance as authorized by The Consolidated Appropriations Act, 2014, Pub. L. No. 113-76, 128 Stat. 5, 62, and as informed by Section 401 of the PRO IP Act. The FY 2014 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.

The competitive grant process ended in March 2014, and in September 2014, OJP announced that it had awarded $2,000,000 in grants to three state and local law enforcement agencies and one non-profit organization in support of the FY 2014 IPEP. The following FY 2014 new 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
2014-ZP-BX-0003	City of Los Angeles (Los Angeles Police Department)[1]	$456,413
2014-ZP-BX-0001	City of Dallas, Texas	$400,000
2014-ZP-BX-0002	County of Essex, New Jersey	$393,587

Since the inception of the program, OJP has awarded $18,480,762 in grants to support state and local law enforcement agencies, training and technical assistance providers, and an IP public education campaign. Of this total amount of funding, state and local enforcement agencies have received $13,549,108. Throughout the duration of the program, these agencies have seized $345,165,300 in counterfeit merchandise; $18,341,026 in other property, and $3,704,294 in currency (total aggregate seizure value: $367,210,620).

In addition to these seizures, grantees achieved the following in the one-year period from July 1, 2013 to June 30, 2014:

[1] The Los Angeles Police Department ("LAPD") is the primary grant recipient. LAPD is formally partnered with the Los Angeles City Attorney's Office in the grant application, and will be providing the City Attorney's Office with grant funds.

- 816 individuals were arrested for violation of IP laws;
- 264 state and local IP search warrants were served; and
- 494 piracy/counterfeiting organizations were disrupted or dismantled.

Examples of how state and local law enforcement used prior IPEP grants include:

- In February 2013, the Sacramento Counterfeit Crime Investigations Team, which is comprised of Sacramento County Sheriff's Detectives and Sacramento FBI agents, conducted four searches in California and targeted six vendors at an area flea market, which yielded 9 arrests and the seizure of over 51,000 CDs; 32,000 DVDs; and $27,908 in cash.

- In March 2013, five individuals were arrested and charged with racketeering, trademark counterfeiting, conspiracy and money laundering in Suffolk County, New York, by the Suffolk County District Attorney's Office. The investigation revealed a sophisticated scheme for importing counterfeit merchandise and labels from China and then distributing the goods to resellers throughout the United States.

- In September 2013, the Los Angeles Police Department ("LAPD"), Anti-Piracy Unit conducted an investigation into the large-scale distribution and sales of counterfeit apparel and accessories. With the assistance of the Southern California IP Task Force (FBI and ICE-HSI), LAPD seized 16,800 counterfeit items totaling over $7,000,000 from two storage units. The distributor ultimately pleaded guilty to 15 state counts of possession and sales of counterfeit goods.

- In February 2014, the Cook County Sheriff's Police and ICE-HSI in Illinois conducted a search of a vehicle diagnostic center and seized 24 counterfeit airbags. The business owner was charged with a state felony count of counterfeit trademarks.

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"). In FY 2014, NW3C conducted these training sessions for 602 attendees from 328 agencies in 31 locations.[2] NW3C also conducted four tailored

[2] Training sessions took place in: Atlanta, GA; Avon Park, FL; Boca Raton, FL; Bronx, NY; Carson City, NV; Gadsden, AL; Georgetown, TX; Hazard, KY; Helena, MT; Las Vegas, NV; Louisville, KY; Manchester, NH; Maywood, IL; Meriden, CT; Meridian, ID; Middletown, VA; Nashville, TN; New York, NY; New York, NY; Newark, DE; Philadelphia, PA; Phoenix, AZ; Pierre, SD; Ponoma, NY; Rancho Cordova, CA; San Diego, CA; San Francisco, CA; Sandy, UT; Santa Fe, NM; St. George, UT.

seminars as well as engaged in additional technical assistance visits to grantee agencies in order to improve their IP investigative and prosecutorial approaches.

Since the inception of the program, BJA has supported the following:

- 76 trainings for 1671 attendees from 889 agencies;
- 9 seminars for 331 attendees from 96 agencies; and
- 15 technical assistance visits for 99 attendees from 28 agencies.

In FY 2014, BJA awarded NW3C a new award of $750,000 to support the continuation of these important trainings and the expansion of training and technical assistance support to jurisdictions engaged in IP enforcement activities to enhance their capacity to respond to IP crime.

(a)(2) Additional Agents of FBI

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

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

(a)(3) FBI Training

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

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

(a)(4) Organized Crime Plan

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

As in FY 2009 through FY 2013, Congress did not appropriate funds to support Section 402(b) of the PRO IP Act in FY 2014.[3] 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 2013, 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 December 2013, representatives of CCIPS organized and presented a training on "Computer Forensics for IP and Health and Safety Crimes" in Nairobi, Kenya. This four-day event brought together approximately 50 law enforcement officials and judges from Kenya, Tanzania, Uganda, Malawi, Mozambique, Angola, Djibouti, and INTERPOL regional office in Harare. The training included methodologies for identifying, preserving, and analyzing digital evidence and also assisted in targeting

[3] 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."

transnational organized crime groups involved in the manufacture and distribution of counterfeit goods.

- In June 2014, representatives of CCIPS and a federal district judge traveled to Mexico City to conduct a training on "Computer Forensics for IP and Health and Safety Crimes." The audience at this five-day event included 50 law enforcement officials and judges from Mexico, Costa Rica, Panama, and the Dominican Republic. The training addressed strategies to target transnational organized crime groups involved in manufacturing and distributing counterfeit drugs as well as how to identify, preserve, triage, and analyze digital evidence.

- In July 2014, representatives of CCIPS presented at a seminar in Mexico City entitled "Advanced Workshop on Effective Enforcement Against Notorious Markets." The workshop—organized by the United States Patent and Trademark Office, the United States Embassy, and the United States Chamber of Commerce—was designed to bring together policy makers, law enforcement experts, and private sector representatives to discuss ways to improve criminal enforcement to better combat Mexican notorious markets. These physical and online marketplaces engage in open sales of pirated and counterfeit goods, and are believed to be connected to transnational and domestic organized crime groups.

(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."*

Section 403 related to funds appropriated during FY2009-13. No funds were appropriated under this section or expended during the reporting period based on funds previously appropriated under this section. Information about the cases, defendants, and types of investigations carried out by the Department may be found described in greater detail below.

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

(a)(6) Other Relevant Information

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

The Department did not receive any authorizations under Sections 401, 402 and 403 of the PRO IP Act in FY 2014.

(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, in FY2014 the Department publically supported changes to the criminal copyright statute to address unauthorized online streaming and modification of Federal Rule of Criminal Procedure 4 to allow for simplified service of foreign corporations in trade secret theft and other cases. Historically, the Department has 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.[4]

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 has participated 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 270 specially-trained federal prosecutors who make up the Department's CHIP program.

[4] For an overview of the Department's policies and efforts in the five years prior to the enactment of the PRO IP Act in October 2008, the Department's PRO IP Act First Annual Report 2008-2009 may be found online at http://www.justice.gov/dag/prioritizing-resources-and-organization-intellectual-property-act-2008. The Department's FY 2010-FY 2013 PRO IP Reports are available at the same location.

CCIPS is a section within the Criminal Division consisting of a specialized team of up to 38 prosecutors who are devoted to enforcing laws related to computer and IP crimes. Thirteen CCIPS attorneys are assigned exclusively to intellectual property enforcement. These attorneys prosecute criminal cases, assist prosecutors and investigative agents in the field, and help develop and implement the Department's overall IP enforcement strategy and legislative priorities. CCIPS attorneys are available to provide advice and guidance to agents and prosecutors on a 24/7 basis. CCIPS attorneys also provide training on 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, working closely with the State Department, recently deployed a new IPLEC to Bucharest, Romania, for Eastern Europe, and will work with the State Department expand the program to an additional three locations in 2015

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.[5] 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") Network 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 representative to the NSCS Network, and in each of the last three years NSCS Network representatives have convened in the D.C. area for specialized training focusing on issues at the intersection of national security and cybersecurity. The NSCS representative provides technical

[5] 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.

and specialized assistance to his or her colleagues within the relevant U.S. Attorney's Office, 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 cybercrimes, and to coordinate and de-conflict national security cyber investigations.

Within NSD, the Counterespionage 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.[6] 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

[6] 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-OCI"), the Department of Commerce's International Trade Administration ("DOC"), the Naval Criminal Investigative Service ("NCIS"), the Defense Criminal Investigative Service ("DCIS"), the Defense Logistics Agency's Office of Inspector General ("DLA"), Immigration and Customs Enforcement's Homeland Security Investigations ("ICE-HSI"), 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's Office of Inspector General ("NASA"), the Department of State's Office of International Intellectual Property Enforcement ("IPE"), the Army Criminal Investigation Command's Major Procurement Fraud Unit ("MPFU"), the Air Force Office of Special Investigations ("AFOSI"), the U.S. Postal Service Office of Inspector General ("USPS OIG"), and the Federal Maritime Commission ("FMC").

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 2014 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 2014, this initiative resulted in a number of significant prosecutions, including those set forth below:

- *Pennsylvania Man Who Sold Counterfeit Military Goods Sentenced To 21 Months In Prison.* On April 17, 2014, Hao Yang, age 25, of Bloomsburg, Pennsylvania, was sentenced to 21 months in prison for conspiring to traffic in counterfeit goods and counterfeit military goods. Yang and his co-conspirators created and operated several companies in Maryland, Pennsylvania, and elsewhere. Yang received counterfeit goods, including counterfeit military-grade circuits, from China, and then shipped the items to buyers in the United States. The counterfeit circuits that Yang redistributed could have caused serious bodily injury or impaired military operations, personnel or national security. Yang pleaded guilty in January 2014, and his guilty plea was the first conviction under the trafficking in counterfeit military goods provision in 18 U.S.C. § 2320, which was passed as part of the National Defense Authorization Act of 2011. (DMD, ICE-HSI)

- *Automotive Parts Supplier Sentenced for Selling Counterfeit Replacement Parts.* On April 30, 2014, Richard Dininni, 57, of Easton, Pennsylvania, was sentenced to eight months incarceration followed by two years of supervised release for conspiring to traffic in counterfeit goods. Dininni operated Professional Parts USA in Easton, Pennsylvania, where he repackaged and sold aftermarket automotive parts, including brakes, anti-lock braking sensors, and suspension air springs, all misrepresented as being produced by original equipment manufacturers such as Ford Motor Company and General Motors. Dininni and two other defendants sold the counterfeit replacement parts, which did not meet independent federal safety standards, to individuals and automotive repair shops. (SDNY, FBI)

- *Pakistani Man Sentenced in Counterfeit Pharmaceutical Case.* On May 2, 2014, Mohammed Jamal Rashid, 45, originally from Pakistan and residing in Houston, Texas, was sentenced to 27 months in prison for conspiracy related to the illegal importation and

attempted trafficking of counterfeit drugs, and receiving and delivering misbranded drugs. Rashid pleaded guilty in January 2014, and admitted he conspired to illegally import counterfeit and misbranded Viagra and Cialis to his home in Houston under a false name and with a false declaration waybill. (SDTX, ICE-HSI, FDA-OCI)

- *California Man Sentenced for Conspiracy to Traffic in Counterfeit Drugs.* On May 8, 2014, Ricky Lee Campbell, 60, of Sacramento, California, was sentenced to 41 months in prison for conspiracy to traffic in counterfeit goods. Co-defendant Susan Yvonne Eversoll, 46, of Sacramento, was sentenced to 18 months in prison for the same charge. According to court documents, law enforcement found more than 6,000 counterfeit tablets resembling Viagra and Cialis when the defendants' residences were searched. (EDCA, FBI, Sacramento County Sheriff's Hi-Tech Crimes Task Force).

- *Massachusetts Man Pleads Guilty to Importing and Selling Counterfeit Integrated Circuits from China and Hong Kong.* On June 3, 2014, Peter Picone 41, of Methuen, Massachusetts, pleaded guilty to trafficking in counterfeit military goods. From 2007 through 2012, Picone imported counterfeit integrated circuits from China and Hong Kong and sold them to customers in the U.S. and abroad. Picone sold the chips to contractors knowing that they would be supplied to the United States Navy for use in nuclear submarines. Picone's guilty plea represents the second conviction ever on a charge of trafficking in counterfeit military goods. (DCT, CCIPS & Cybercrime Lab, FRAUD, AFMLS, DCIS, ICE-HSI, NCIS)

- *Rhode Island Man Sentenced for Trafficking in Counterfeit Health and Beauty Products.* On June 19, 2014, Norman Cipriano, 41, of Warwick, Rhode Island, was sentenced to 50 months in federal prison for trafficking more than 14,500 counterfeit health and beauty products, sports jerseys, and clothing accessories valued at more than $1 million dollars. Cipriano pleaded guilty in August 2013 to trafficking in counterfeit goods and services. Pursuant to a search warrant executed in September 2012, law enforcement seized a significant quantity of counterfeit over-the counter medications as well other counterfeit products from Cipriano's home. (DRI, ICE-HSI, Warwick Police)

- *Fourth Circuit Affirms North Carolina Man's Sentence for Trafficking in Counterfeit Airbags.* On June 24, 2014, the U.S. Court of Appeals for the Fourth Circuit affirmed the sentence of Igor Borodin, 27, of Indian Trial, North Carolina. Previously, in October 2013, Borodin was sentenced to 84 months in prison for trafficking in counterfeit goods and 60 months for transporting hazardous material, to run concurrently. Between February 2011 and May 2012, Borodin sold at least an estimated 7,000 counterfeit airbags online, and earned at least $1.4 million dollars in revenue. (WDNC, ICE-HSI, DOT-OIG).

- *Illinois Man Sentenced for Smuggling Counterfeit Viagra Tablets.* On July 17, 2014, Fayez Al-Jabri, 45, of Chicago, Illinois, was sentenced to serve 41 months in prison, and ordered to pay $15,066 in restitution and forfeit $47,750. Al-Jabri previously pleaded guilty in March 2014 to trafficking in counterfeit goods and introducing counterfeit goods into interstate commerce in violation of the Food, Drug and Cosmetic Act, including counterfeit Viagra tablets. According to court documents, Al-Jabri conspired to smuggle more than 26,000 Viagra tablets from China into the United States for further distribution. (SDTX, CCIPS, ICE-HSI, FDA, DSS, Houston PD, Chicago PD)

- *Turkish Man Pleads Guilty to Smuggling Counterfeit Cancer Drugs.* On July 22, 2014, Ozkan Semizoglu, the "Foreign Trade Director" of a Turkish drug wholesaler, pleaded guilty to smuggling counterfeit, misbranded and adulterated cancer treatment drugs into the United States, including multiple shipments of Altuzan (the Turkish version of Avastin). Co-defendant Sabahaddin Akman previously pleaded guilty to similar charges. To further their scheme, defendants falsely labeled and declared the cancer drugs, which they then imported from Turkey. Additionally, Defendants knowingly shipped the climate-sensitive drugs without proper temperature control, endangering users of the counterfeit drug. In October 2014, Semizoglu was sentenced to 27 months in prison. (EDMO, DPR, FDA, USMS, HHS OIG, Johnson County Crime Lab)

- *Two Individuals Plead Guilty to Importing and Selling Hazardous and Counterfeit Toys in New York.* On August 27, 2014, Chenglan Hu, 52, and Hua Fei Zhang, 53, of Bayside, New York, pleaded guilty in connection with importing children's toys with copyright-infringing images and counterfeit trademarks of popular children's characters, as well as unsafe lead levels, small parts that presented choking risks, easily-accessible battery compartments, and other potential hazards. Hu and Zhang were the last of nine defendants to plead guilty for conduct relating to the import scheme. The defendants used companies they owned to import toys from China and sell them throughout New York. (EDNY, CCIPS, EDNY, ICE-HSI, NYPD, CPB, CPSC)

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

In FY 2014, 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:

- *South Carolina Engineer Indicted for Stealing Trade Secrets.* On October 24, 2013, Yi Liu, 40, of Lexington, South Carolina, was charged with stealing trade secrets from Sprung-brett RDI, a technology firm in Amhert, New York. Liu, a former engineer with Sprung-brett, also was charged with unlawfully accessing a Sprung-brett computer, the interstate transportation of stolen property, and wire fraud. The trade secret information at issue relates to electric actuation system technology, which Sprung-brett was developing for possible use in nuclear submarines and on Air Force fighter jets. (WDNY, FBI)

- *Two Agricultural Scientists Charged With Stealing Trade Secrets.* On December 18, 2013, Weiqiang Zhang, 47, Manhattan, Kansas, and Wengui Yan, 63, Stuttgart, Arkansas, both agricultural scientists from China, were charged with conspiracy to steal trade secrets and theft of trade secrets. Specifically, the indictment alleges that as part of the conspiracy, Zhang and Yan enabled visitors from a Chinese crops research institute to obtain possession of the unique rice seeds developed by Ventria Bioscience at a Kansas facility. (DKAN, CCIPS, FBI, CBP)

- *Executive Recruiter Sentenced for Trade Secret and Computer Intrusion Charges.* On January 8, 2014, David Nosal, 55, of Danville, California, was sentenced to one year and one day in prison. Subsequently, on May 29, 2014, the judgment for Nosal, a former employee of executive search firm Korn/Ferry International, was amended to include a restitution order of $827,983.25. In April 2013, a federal jury convicted Nosal 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. (NDCA, CCIPS, FBI)

- *Michigan Engineer Sentenced for Stealing Trade Secrets.* On January 16, 2014, Michael Agadoa, 62, of Midland, Michigan, was sentenced to two years in prison after having pleaded guilty to stealing trade secrets. Agadoa, who worked for Wacker Chemical Corporation as an engineer for a number of years, admitted that he took trade secret information related to the production of Wacker's silicone-based and rubber products when he left the company's employment in 1997. He then used this trade secret information, in early 2010, to negotiate employment with a Korean-based chemical company, KCC Silicones, and from March 2010 to April 2012, to assist KCC in the development of silicone-based products. (EDMI, FBI)

- *Four Members of International Computer Hacking Ring Indicted for Stealing Gaming Technology and Apache Helicopter Training Software.* On April 23, 2014, four members of an international computer hacking ring, Nathan Leroux, 20, of Bowie, Maryland; Sanadodeh Nesheiwat, 28, of Washington, New Jersey; David Pokora, 22, of Mississauga, Ontario, Canada; and Austin Alcala, 18, of McCordsville, Indiana, were charged in the District of Delaware with conspiracies to commit computer fraud, copyright infringement, wire fraud, mail fraud, identity theft and theft of trade secrets, as well as with individual counts of similar conduct. According to court records, from January 2011 to March 2014, the defendants allegedly hacked into the computer networks of Microsoft Corporation, Epic Games Inc., Valve Corporation, Zombie Studios and the U.S. Army. The value of the intellectual property and data that the defendants stole, as well as the costs associated with the victims' responses to the crimes, is estimated to range between $100 million and $200 million. On September 30, 2014, Pokora and Nesheiwat pleaded guilty to conspiracy to commit computer fraud and copyright infringement. (DDE, CCIPS, OIA, FBI, ICE-HSI, CBP, USPIS)

- *Chinese National Arrested for Conspiring to Steal Trade Secrets.* On July 1, 2014, Mo Yun, a Chinese national previously employed by Beijing Dabeinong Technology Group Company ("DBN") was arrested and indicted for conspiracy to steal trade secrets from several U.S. based seed manufacturing companies, and transport those trade secrets to China for the benefit of their China-based seed company. Co-conspirator Mo Hailong was previous arrested in December 2013. DBN is believed to be a Chinese conglomerate with a corn seed subsidiary company, Kings Nower Seed. (SDIA, FBI)

- *Toray Chemical Resolves Attempted Theft of Trade Secrets Investigation and Agrees to Pay Over $2 Million Penalty.* On July 9, 2014, a criminal information was filed against Toray Chemical Korea, Inc. and a two-year deferred prosecution agreement was filed in the U.S. District Court for the Eastern District of Virginia. The company agreed to pay a criminal penalty of over $2 million to resolve an attempted theft of trade secrets investigation

involving the theft of meta-aramid fiber technology. Meta-aramid fibers are used in a variety of applications, including protective fabrics, electrical insulation and lightweight structural support for commercial aircraft. (EDVA, FBI)

- *California Businessman Sentenced to 15 years for Selling DuPont's Secrets.* On July 10, 2014, California businessman Walter Liew was sentenced to 15 years in prison for stealing manufacturing secrets from DuPont Company and selling the information to Chinese-owned companies. In May 2014, a federal jury found Liew, his company USA Performance Technology Inc., and Robert Maegerle guilty of economic espionage, theft of trade secrets, bankruptcy fraud, tax evasion, and obstruction of justice for their roles in a long-running effort to obtain U.S. trade secrets for the benefit of companies controlled by the Chinese government. The jury found the defendants conspired to steal DuPont trade secrets and sold those secrets for large sums of money to Chinese state-owned companies. (NDCA, NSD, FBI, IRS)

- *Sixth Circuit Affirms Defendants' Convictions and Sentences for Conspiracy to Steal GM Trade Secrets.* On July 26, 2014, the U.S. Court of Appeals for the Sixth Circuit affirmed the sentences for Shanshan Du, 51, and her husband, Yu Qin, 49, of Troy, Michigan. Following a jury trial, Du was sentenced to one year and one day in prison and fined $12,500, and Qin was sentenced to three years in prison and fined $25,000. Defendants also were ordered to forfeit $279,406.50. While employed with GM, Du stole GM trade secret information relating to hybrid vehicles to benefit Millennium Technology International Inc. (MTI), a private company owned by the defendants. MTI then provided the stolen trade secrets to Chery Automobile, a China-based automotive manufacturer. GM estimated that the value of the stolen trade secret information was more than $40 million. (EDMI, FBI)

- *Los Angeles Grand Jury Indicts Chinese National in Computer Hacking Scheme Involving Theft of Military Trade Secrets.* On August 14, 2014, a federal grand jury indicted Chinese national Su Bin, 49, on five felony offenses stemming from a computer hacking scheme that involved the theft of trade secrets from American defense contractors, including The Boeing Company. The indictment alleges that Su worked with two unindicted co-conspirators based in China to infiltrate computer systems and obtain confidential information about military programs, including the C-17 transport aircraft, the F-22 fighter jet, and the F-35 fighter jet. The indictment specifically alleges three charges related to unauthorized computer access, a conspiracy to illegally export defense articles and a conspiracy to steal trade secrets. (CDCA, FBI, AFOSI)

(3) Large-Scale Commercial Counterfeiting and Online Piracy

The Department continues to pursue significant, large-scale piracy and counterfeiting operations. In FY 2014, the Department has had a number of si*g*nificant prosecutions, including those set forth below:

- *Three Different Android Mobile Device App Piracy Groups Prosecuted.* In each case, leading members of Android mobile device app piracy groups were charged with renting computer servers to host websites such as www.snappzmarket.com, www.appbucket.net, and www.applanet.net, and with providing digital storage for the pirated copies of copyrighted

Android apps that each group distributed to their members or subscribers. Seizure orders were executed against these three website domain names for the illegal distribution of copies of copyrighted Android mobile device apps – the first time website domains involving mobile device app marketplaces have been seized. **(**NDGA, CCIPS, FBI, CCIPS & Cybercrime Lab, OIA)

- *First Ever Charges Filed Against Members of Mobile Device App Piracy Group.* On January 23, 2014, Kody Jon Peterson, 22, of Clermont, Florida, a leading member of the SnappzMarket Group, was charged by information with conspiracy to commit criminal copyright infringement. He pleaded guilty to the information in April 2014. On July 17, 2014, an indictment was unsealed charging other members of the SnappzMarket Group, Gary Edwin Sharp II, 26, of Uxbridge, Massachusetts, Joshua Ryan Taylor, 24, of Kentwood, Michigan, and Scott Walton, 28, of Cleveland, Ohio, with criminal copyright infringement. From May 2011 through August 2012, the defendants and others conspired to reproduce and distribute over one million copies of copyrighted Android mobile device apps, with a total retail value of over $1.7 million. In November 2014, Walton pleaded guilty for his role in the conspiracy.
- *First Ever Convictions Obtained Against Members of Mobile Device App Piracy Group*. On January 24, 2014, Nicholas Anthony Narbone, 26, of Orlando, Florida, Thomas Allen Dye, 21, of Jacksonville, Florida, and Thomas Pace, 38, of Oregon City, Oregon, leading members of the Appbucket Group, were charged by information with conspiracy to commit criminal copyright infringement. Narbone and Dye pleaded guilty in March 2014, and Pace pleaded guilty in April 2014. In addition, on July 17, 2014, an indictment was unsealed charging another Appbucket Group member, James Blocker, 36, of Rowlett, Texas with conspiracy to commit criminal copyright infringement. From August 2010 to August 2012, the Appbucket Group reproduced and distributed over one million copies of copyrighted Android mobile device apps, with a total retail value of over $700,000.
- *Members of Applanet Android Mobile Device App Piracy Groups Charged.* On July 17, 2014, an indictment was unsealed charging Aaron Blake Buckley, 20, of Moss Point, Mississippi, David Lee, 29, of Chino Hills, California, and Gary Edwin Sharp II, who was also indicted with the SnappzMarket Group, with conspiracy to commit criminal copyright infringement and other similar crimes. From May 2010 through August 2012, the defendants conspired with others to reproduce and distribute over 4,000,000 copies of copyrighted Android mobile device apps, with a total retail value of over $17 million.

- *Five Defendants Indicted for Scheme to Defraud Consumers Through the Sale of Counterfeit Luxury Goods.* On February 3, 2014, Joseph Mosseri, 43, Albert Mosseri, 34, Oded Hakim, 46, Elliott Shasho, 41, and Andrew Li, 34, all of Brooklyn, New York, were charged for their alleged participation in a scheme that victimized hundreds of consumers and numerous credit card processors through the online marketing and sales of counterfeit luxury handbags. According to the indictment, the defendants and others controlled a series of websites that sold luxury fashion items and accessories, advertising that the goods were authentic but offered at a discount because of manufacturing defects. In fact, the defendants either never shipped the goods to customers or shipped counterfeit goods. The defendants also defrauded

the credit card processors by misrepresenting the reasons for disputed charges and obstructing efforts by credit card processors to recover disputed funds. (SDNY, USPIS, ICE-HSI, CBP, NY Dept of Taxation and Finance)

- *Chinese Nationals Sentenced in Counterfeit Sneaker Case.* On February 25, 2014, Huang Yue Feng, 33, of Queens, New York, and Wang He Bin, 31, of Franklin Square, New York, were sentenced to 12 months in prison for conspiracy to traffic in counterfeit goods. The defendants also forfeited over $400,000 in cash and property seized during the execution of search warrants at New York City warehouses. Feng and Ben were involved in the importation of counterfeit Nike sneakers from China, which were then distributed throughout the United States. The defendants are among 23 individuals charged in the counterfeiting scheme; 22 defendants were convicted and one defendant was acquitted after an October 2012 trial. (WDNY, ICE-HSI).

- *California Man Sentenced to Prison for Counterfeit Media Conspiracy.* On March 3, 2014, Leonel Martinez Caballero, 31, of Modesto, California, was sentenced to four years in prison for his November 2013 guilty plea to conspiracy to commit criminal copyright infringement and traffic in counterfeit labels and counterfeit documentation and packaging. In 2011, Caballero was involved in an extensive scheme with others to store and distribute counterfeit CDs and DVDs. Caballero managed a warehouse in Modesto that served as a distribution point for counterfeit media; approximately 100,000 counterfeit CDs and DVDs were found inside the warehouse. (EDCA, FBI, Sacramento Valley Hi-Tech Crimes Task Force).

- *Importer of Fake Brand Name Goods Sentenced.* On May 8, 2014, Kevin "Peter" Wang, 54, of Rosemead, California, who coordinated the importation of 11 containers of counterfeit apparel – including Nike, Gucci and Coach products worth more than $2.3 million – was sentenced to 31 months in prison. From 2008 to 2012, Wang participated in a large-scale smuggling operation, helping Chinese exporters smuggle counterfeit goods into the United States through the ports of Los Angeles and Long Beach. (CDCA, ICE-HSI)

- *Members of Largest Counterfeit Goods Conspiracy Ever Sentenced.* On June 23, 2014, Hai Dong Jiang, 37, of Staten Island, and Ming Zheng, 48, of New York, were sentenced to 120 months and 46 months in prison, respectively. From November 2009 through February 2012, Jiang, Zheng and seven others ran one of the largest counterfeit goods smuggling and distribution conspiracies ever charged by the Department of Justice. The defendants and others conspired to import hundreds of containers of counterfeit goods – primarily handbags, footwear, and perfume – from China into the United States. The goods, if legitimate, would have had a retail value of more than $300 million. The counterfeit goods, which were manufactured in China, were smuggled into the United States through containers fraudulently associated with legitimate importers, with false and fraudulent shipping paperwork playing a critical role in the smuggling scheme. (DNJ, ICE-HSI, FBI)

- *California Man Sentenced for Copyright Infringement Conspiracy.* On July 23, 2014, Otto Godinez-Sales, 22, of San Jose, California, was sentenced to four years in prison for conspiracy to commit criminal copyright infringement. Godinez-Sales maintained a number of warehouses in the San Jose area where he sold counterfeit CDs and DVDs to customers, including two co-defendants who would transport the CDs and DVDs to sell at area flea markets. In many instances, the copyrighted movies being trafficked by the defendants were

still in theatrical release and not yet available for purchase in the home DVD market. (EDCA, FBI, Sacramento Valley Hi-Tech Crimes Task Force).

- *Washington Company, Owner, and Sales Manager Sentenced for Trafficking in Counterfeit Goods.* On September 19, 2014, a Washington company, Connectzone.com, LLC, its owner, Daniel Oberholtzer, 50, of Lynnwood, and a sales manager, Warren Lance Wilder, 46, of Auburn, Washington were resentenced. Oberholtzer and Wilder were sentenced to 37 and 33 months imprisonment, respectively, and Connectzone was sentenced to five years probation. Previously, in April 2014, a jury convicted Wilder of conspiracy to traffic in counterfeit goods, mail fraud, and trafficking in counterfeit goods, and in February 2014, Oberholtzer and his company pleaded guilty to conspiracy to traffic in counterfeit goods. Connectzone.com had websites that advertised and sold counterfeit Cisco computer networking products obtained from multiple foreign suppliers of counterfeit goods, including the Chinese company Xiewei Electronics. (WDWA, ICE-HSI, Seattle-Tacoma Border Enforcement Security Task Force).

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 2014, the Department 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 New York, New York (November 2013); Nashville, Tennessee (February 2014); Riverside County and Sacramento, California (March 2014); Mobile, Alabama (June 2014); Buffalo, New York (June 2014); Saint Paul, Minnesota (August 2014); and Pearl, Mississippi (August 2014).

- In September 2014, 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, cybercrimes, IP crimes, and other topics.

- In November 2013, NSD, with support from CCIPS, organized and led the annual 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 annual CHIP conference to address the added complexity of working with classified information and related issues to investigate, prosecute, and otherwise disrupt those crimes.

- In February 2014, CCIPS organized and taught the IP Seminar at the NAC in Columbia, South Carolina. This seminar, which was attended by approximately 50 prosecutors and federal agents, provided substantive instruction on trademark counterfeiting, copyright piracy, and trade secret theft through case studies, as well as in-depth guidance regarding online investigations and digital forensics.

- In February 2014, 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, focused on the technical and legal issues surrounding the analysis of seized digital media.

- In March 2014, CCIPS organized and taught the Complex Online Crime Seminar at the NAC in Columbia, South Carolina. This seminar, which was attended by approximately 50 prosecutors, used a case scenario involving IP crime to provide a number of strategies and techniques for investigating criminal offenses occurring over the Internet.

- In July 2014, CCIPS trained approximately 50 FBI agents as part of the IPR Center's three-day conference on IP enforcement.

- 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 2014 in locations such a Los Angeles, CA; Lansing, MI; Lakewood, WA; and Boston, MA. 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 the government shutdown and budgetary constraints, in FY 2014 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 2014 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. In FY 2014, an experienced CHIP attorney continued his service as the third IP Law Enforcement Coordinator ("IPLEC") in Bangkok, Thailand. Another experienced CHIP attorney will begin service as the Eastern Europe IPLEC in January 2015 (a role that has been vacant since 2011). Additionally, DOJ continued to engage with China through the bilateral IP Criminal Enforcement 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 November 2013, CCIPS attorneys participated in the 11th Annual Meeting of the Joint Liaison Group on Law Enforcement Cooperation ("JLG") in Washington, D.C. The JLG is designed to strengthen law enforcement cooperation between the United States and China across a range of issues, including intellectual property and cybercrime. As co-chair, CCIPS' Deputy Chief led the IPCEWG meeting, which was held alongside the plenary JLG session and included a discussion of the identification of new initiatives for cooperation. 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. Also in attendance at the JLG meeting were additional representatives from DOJ, DOS, FBI, and ICE.

Meetings with Chinese Government Delegations. During FY 2014, CCIPS attorneys participated in a number of meetings with visiting Chinese government officials. These meetings include: February 2014 meeting with five representatives from various Chinese government agencies at CCIPS as part of the Department of State's International Visitor Leadership Program; June 2014 meeting with 20 officials from the Jiangsu Province's IP Office at the U.S. Patent & Trademark Office's Global Intellectual Property Academy ("USPTO's GIPA"); September 2014 meeting with more than 20 Chinese IP officials at the USPTO's GIPA as part of the IP Working Group meeting of the U.S.-China Joint Commission on Commerce and Trade; September 2014 meeting with approximately 15 Chinese government officials from various agencies and the judiciary at the USPTO- and USTR-sponsored Bilateral Exchange Program on IP Legislation, Regulation, Judicial Interpretation held at the USPTO's GIPA.

AFRICA

Combating IP Crime Training in Morocco. In November 2013, CCIPS trained approximately 40 prosecutors, investigators, and judicial officials at an IPR colloquium in Casablanca, Morocco. The workshop was sponsored by the USPTO and the Moroccan Office of Industrial and Commercial Property. CCIPS provided training regarding lead development, working with rights holders, evidentiary issues, and charging decisions in IP investigations.

IP Enforcement and Computer Forensics Training in Kenya. In December 2013, CCIPS organized and presented a training on "Computer Forensics for IP and Health and Safety Crimes" in Nairobi, Kenya, for 50 law enforcement officials and judges from Kenya, Tanzania,

Uganda, Malawi, Mozambique, Angola, Djibouti, and the INTERPOL regional office in Harare, Zimbabwe. The training included methodologies for identifying, preserving, triaging, and analyzing digital evidence and also assisted in targeting transnational organized crime groups involved in the manufacture and distribution of counterfeit goods.

Criminal Enforcement Assessment in Senegal. In December 2013, CCIPS traveled to Dakar, Senegal, to conduct an IP criminal enforcement assessment mission with the United Nations Office on Drugs and Crime and various law enforcement officials. The assessment was the first step in implementing joint trainings between DOJ and UNODC in Africa to better address issues related to IP and organized crime, to see how future DOJ capacity-building events can take advantage of the UNODC Container Control Program at the ports, and to use UNODC's structure in the region to monitor the effectiveness of DOJ trainings

IP Enforcement Training in Ghana. In February 2014, CCIPS helped teach an ICE-sponsored weeklong course in IP rights enforcement in Accra, Ghana, for approximately 30 prosecutors, police, customs officers, and other government officials from Ghana, Nigeria, and the Gambia. CCIPS presented on various topics, including investigating and prosecuting counterfeit hard goods cases, fake medicines, internet piracy and cybercrime, international cooperation and information sharing, and case studies and best practices.

Sub-Saharan Africa Fraudulent Drug Training. In June 2014, a representative from the Consumer Protection Branch ("CPB") gave a presentation on "Investigating and Prosecuting Pharmaceutical Crime" at Sub-Saharan Africa Fraudulent Drug Training hosted by the USPTO's GIPA. The training was attended by drug regulators, customs, and law enforcement officials from Tanzania, Angola, South Africa, Namibia, Zambia, Mozambique, and Botswana.

IPR Enforcement Training in Togo. In August 2014, CCIPS facilitated a workshop organized by ICE on "Intellectual Property Rights Enforcement Training" in Lomé, Togo. The workshop gathered prosecutors, investigators, customs officers, and other IP law enforcement officials from Togo, Benin, Cote d'Ivoire, and Senegal. To help increase cooperation, representatives from Ghana and Nigeria were also present. CCIPS' involvement in the Workshop assisted with the Department's mission to bolster criminal enforcement of IP in African French-speaking countries.

MEXICO

Capacity-Building and Cooperation with Mexican Customs Authorities. In October and November 2013, CCIPS organized and conducted assessments in Panama City, Panama, and San Jose, Costa Rica, of regional capacity-building workshops that would increase cooperation with the Mexican authorities and address trans-shipments of counterfeit goods through Mexico to other countries in the region.

Train-the-Trainer Program for Criminal IP Enforcement in Mexico. In January 2014, CCIPS facilitated the first phase of a workshop on drafting training materials for criminal IP enforcement at the border in Pueblo, Mexico. The workshop developed training modules that will allow Mexican officials (previously prepared by DOJ and by the World Customs

Organization ("WCO")) to train customs officers and prosecutors in Mexico as well as elsewhere in the region on customs issues affecting criminal enforcement of IP.

IP Regional Workshops for Enforcement Agencies. In March and April 2014, with the assistance of the USPTO and the WCO, CCIPS organized and facilitated regional workshops on "Interagency Cooperation for Criminal Enforcement of Intellectual Property at the Border" in San Jose, Costa Rica, and in Panama City, Panama. The workshops included 50 officials from Mexico, Costa Rica, and Panama representing customs, IP, and health and safety agencies, as well as prosecutors.

Advanced IP Training for Five Latin American Countries. In June 2014, CCIPS participated in a weeklong symposium addressing advanced topics and techniques in prosecuting IP crimes. The 40 participants were from Mexico, El Salvador, Honduras, Costa Rica, and Brazil, and instructors were from CCIPS, DHS, FDA, and the pharmaceutical industry. The training was sponsored by the IPR Center and International Law Enforcement Academy.

Computer Forensics Training in Mexico. In June 2014, CCIPS presented a training on "Computer Forensics for Intellectual Property and Health and Safety Crimes" in Mexico City, Mexico. The audience included 50 law enforcement officials and judges from Mexico, Costa Rica, Panama, and the Dominican Republic. The course addressed how to identify, preserve, triage, and analyze digital evidence, as well as how to target transnational organized crime groups involved in the manufacture and distribution of counterfeit goods

CCIPS Presents Workshop on IP Criminal Enforcement. In July 2014, CCIPS presented a seminar in Mexico City, Mexico, entitled "Advanced Workshop on Effective Enforcement Against Notorious Markets." Organized by the USPTO, the U.S. Embassy, and the U.S. Chamber of Commerce, the workshop was designed to bring together policy makers, law enforcement experts from the Mexican Attorney General's office and federal police, and private sector representatives to discuss ways to improve criminal enforcement to better combat Mexican notorious physical and online markets, which engage in open sales of pirated and counterfeit goods.

OTHER REGIONS

IP Training at ILEA in Thailand. In October 2013, CCIPS traveled to Bangkok, Thailand, to serve as an instructor at a seminar on the investigation and prosecution of IP crimes. The ICE-organized seminar was held at the International Law Enforcement Academy ("ILEA"). Attendees included law enforcement officials and prosecutors from Thailand, Cambodia, Laos, Timor-Leste, the Philippines, Hong Kong, Indonesia, Vietnam, and Malaysia.

IP Enforcement Training Program at ILEA in San Salvador. In February 2014, the ILEA in San Salvador, El Salvador hosted a weeklong course on IP enforcement for approximately 30 police, prosecutors, forensic experts, customs officers, and other government officials from Chile, Colombia, El Salvador, Paraguay, and Uruguay. ICE sponsored the training, which included instruction from CCIPS on a number of topics, including combating counterfeit pharmaceuticals, internet piracy and cybercrime as well as international cooperation and information sharing.

IP Enforcement Course at ILEA in Budapest. In March 2014, CCIPS helped teach a weeklong course on IP enforcement at the ILEA in Budapest, Hungary. Approximately 35 prosecutors, police, customs officers, and IP inspectors from Bulgaria, Romania, and Ukraine attended the ICE-sponsored training.

IP Enforcement Program at ILEA in Peru. In April 2014, CCIPS participated in and presented at an IP enforcement training sponsored by ICE at the ILEA in Lima, Peru. The program brought together experienced police, prosecutors, and customs officials from Chile, Colombia, and Peru for training on the investigation and prosecution of criminal intellectual property cases, identification of pirated and counterfeit goods, and digital investigative techniques.

Counterfeit Medicine Conference for Government Officials. In May 2014, a CPB representative spoke on a panel in Washington, D.C., at the French Embassy's conference entitled "Trafficking and Counterfeiting of Medicines: A Toolkit for Investigators." The conference was sponsored by the French customs, police, justice, and IPR attachés, and attended by customs, law enforcement, justice, and regulatory officials from many different countries, including the United States, France, Australia, Canada, New Zealand, India, and China. Other speakers and attendees were from Europol, INTERPOL, the IPR Center, the International Anti-Counterfeiting Coalition, and the pharmaceutical industry.

IPR Training Conferences for Ukrainian Officials. In September 2014, CCIPS helped teach two two-day IP training workshops in Kyiv, Ukraine on internet piracy issues for about 50 Ukrainian judges, prosecutors, police, IP inspectors, other government officials, and rights holders. The U.S. Department of Commerce initiated and sponsored the training.

INTERPOL IP Crime Conference in Vietnam. In September 2014, CCIPS presented at INTERPOL's 2014 International Law Enforcement IP Crime Conference in Hanoi, Vietnam. The conference brought together over 600 law enforcement and customs personnel from 83 countries to gain an international perspective on the trade in counterfeit and pirated products, to share international best practices, and to provide a global forum for networking and partnership development.

CCIPS Meets with Delegates of 25 Countries. Throughout FY 2014, CCIPS participated in a wide-range of programs and meetings for international visitors from more than 25 countries to engage on IP enforcement issues. Visiting delegations included representatives from Afghanistan, Armenia, Brazil, Canada, Chile, China, India, Indonesia, Italy, Japan, Jordan, Kenya, Morocco, Nigeria, Pakistan, Paraguay, Singapore, South Korea, Sri Lanka, Thailand, Turkey, Tunisia, Ukraine, United Arab Emirates, and Vietnam. Programs included a January 2014 roundtable with Thai judges held at the U.S. Copyright Office; a January 2014 seminar for Canadian law enforcement officers held at the IPR Center; an April 2014 International Visitors Program meeting with 13 government officials and other stakeholders from a wide range of countries; a May 2014 meeting with copyright experts from 16 different countries at the U.S. Copyright Office; a May 2014 meeting with Armenian IP officials, a July 2014 meeting with South Korean IP officials, an August 2014 workshop with Indian investigators, and a September 2014 presentation for Pakistani and Sri Lankan IP officials, all held at the USPTO's GIPA.

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 IP Industry and Law Enforcement Meeting in September 2014, in Washington, D.C. The yearly meeting provides 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 Attorney General Eric Holder and Assistant Attorney General Leslie Caldwell. Senior law enforcement officials from DOJ, FBI, ICE, and FDA participated in the meeting. More than 90 individuals attended the meeting, including senior representatives from a broad range of industries such as pharmaceuticals, software, luxury goods, electronics, apparel, motion pictures, music, 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: Practicing Law Institute Conference on IP Enforcement in New York, in January 2014; American Bar Association's Section of Public Contract Law Panel Discussion in Washington, D.C., in February 2014; U.S. Telecommunications Training Institute Seminar in Washington, D.C., in April 2014; the Underwriters Laboratory Brand Protection Workshop in Los Angeles, California, in June 2014; the FBI and InfraGard's Organizational Espionage and Insider Threat conference in Minneapolis, Minnesota, in July 2014; Homeland Security Investigations Brand Protections Workshop in Houston, Texas, in August 2014.

During FY 2014, CCIPS and the IPR Center co-hosted two meetings of the Counterfeit Microelectronics Working Group, which focuses on the challenge of counterfeit microelectronics in the government supply chain and related issues. Over 50 representatives from the microelectronics industry and law enforcement attended the April 2014 meeting, and over 80 representatives attended the September 2014 meeting.

In addition to these Counterfeit Microelectronics Working Group meetings, CCIPS attorneys participated in the U.S. Space Programs Mission Assurance Workshop in Chantilly, Virginia, in May 2014. The workshop addressed anti-counterfeiting guidance and reporting requirements triggered when counterfeit components are identified. A CCIPS attorney also presented at the June 2014 Symposium on Counterfeit Electronic Parts and Electronic Supply Chain in College Park, Maryland. This symposium is the leading forum in the country regarding technology and policy developments in the area of electronics supply chain and counterfeit electronics prevention

Similarly, NSD leadership and other attorneys have reached out to senior managers at more than 50 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 universities and think tanks, including Assistant

Attorney General John Carlin's presentation on cybercrime at Carnegie Mellon University in July 2014, as well as 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 and facilitated FBI field offices' efforts to educate AUSAs on the threat of economic espionage in their districts and to include them in FBI's outreach efforts in their districts.

On December 12, 2013, CCIPS attorneys participated along with two FBI Supervisory Special Agents in a panel discussion on theft of trade at the IPR Center's annual symposium. This year's symposium was entitled "Innovative and Unique Strategies for IP Protection."

On April 3, 2014, a senior CCIPS official spoke at the ABA's Annual Intellectual Property Law Spring Conference in Washington, D.C., regarding developments in federal criminal law concerning the theft of trade secrets and factors federal prosecutors consider in deciding whether to accept a trade secret case for prosecution.

On May 8, 2014, a CCIPS attorney presented on criminal enforcement of trade secret law as part of the Defense Research Institute's two day Business Litigation Seminar.

On June 11, 2014, a senior CCIPS official delivered a keynote address at the 2014 Chief Legal Officer Leadership Forum, which included the top legal officers for many of the largest companies in the country. CCIPS presented on emerging cybercrime and IP threats, developments in law enforcement's response, and ways in which the government and private sectors can work together to minimize and respond to these threats.

On September 18, 2014, a CPB senior litigation counsel moderated a panel discussion by AUSAs at the Partnership for Safe Medicines Interchange. The Interchange is an annual symposium for policymakers, healthcare professionals, patient advocates, law enforcement, pharmaceutical manufacturers, and anti-counterfeiting companies to discuss the problems and solutions to the global problem of pharmaceutical crimes, including counterfeit, misbranded, unapproved, and adulterated drugs and devices. The panel addressed patient safety issues encountered with these crimes and issues faced in prosecuting these cases.

On September 23, 2014, a CCIPS attorney presented at a meeting of the Office of the Director of National Intelligence's Trade Association Partners. The presentation addressed best practices for preventing and responding to computer crimes and IP theft. In attendance were a wide range of attorneys and representatives of industry, including national leaders of trade associations.

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 sites can be found at http://www.justice.gov/dag/iptaskforce/ and http://www.cybercrime.gov/ (also linking the IPR Center http://www.iprcenter.gov/).

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 $80.4 million in donated media, including more than 77,765 total airings on television in 209 of 210 nationwide markets and 22,895 airings on radio. In addition, 1,841 digital mall posters have been displayed in 43 nationwide markets; print support for the campaign continues to be strong, adding another $412,000 in donated media for this past year.

In 2013 and 2014, NCPC traveled to Connecticut, Texas, and California to conduct IP training for IPEP grantees, and to share the public education campaign and discuss strategies for local law enforcement's use of the campaign products. NCPC also delivered IP training to, and shared the campaign with, local law enforcement in Utah. In addition, NCPC provided campaign materials to IP trainings in Lansing, MI; Pittsburgh, PA; Myrtle Beach, SC; and Columbus, OH, all of which were conducted by NW3C and NAAG.

NCPC continues to work directly with prior IPEP grantees in Baltimore, Orlando, and Los Angeles to localize announcements from the campaign for use in their communities. Specifically, NCPC worked with the Baltimore Police Department to develop an IP educational brochure and provided posters, palm cards, and fliers for the department to use in its community efforts. The city of Orlando requested our help in localizing two of the posters from the IP campaign. Additionally, NCPC partnered with the Deputy City Attorney in Los Angeles to localize and record Spanish-language versions of the IP radio PSAs.

(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. 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. 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 FY 2014, listing the number of defendants and cases charged, the number of defendants sentenced, and the length of those sentences.[7] Section 404(b) of the PRO IP Act

[7] Case statistics were compiled by the Executive Office of the United States Attorneys ("EOUSA"). The chart includes data on criminal cases/defendants where the following charges were brought as any charge against a defendant: 17 U.S.C. §506 (criminal copyright infringement); 17 U.S.C. §§ 1201 to 1205 (circumvention of copyright protection systems); 18 U.S.C. §§ 1831 (economic espionage) & 1832 (theft of trade secrets); 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 (cont'd)

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.

District Totals	FY2014
Investigative Matters Received by AUSAs	256
Defendants Charged	200
Cases Charged	142
Defendants Sentenced	184
No Prison Term	92
1-12 Months	30
13-24 Months	30
25-36 Months	14
37-60 Months	13
60 + Months	5

In addition, we have provided the chart below with FY2014 statistics for criminal IP cases broken down by type of charge.[8]

Charge	Cases charged	Percentage
Trademark *Trafficking in counterfeit goods, 18 U.S.C. § 2320*	91	59.9%
Copyright *Criminal copyright infringement, 17 U.S.C. §506 & 18 U.S.C. § 2319*	45	29.6%

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.

[8] EOUSA compiled the statistics for number of cases charged broken down by IP statute. These statistics may not reflect cases where only a conspiracy to violate one of these offenses was charged, and there may be double-counting of cases where more than one statute was charged in the same case.

Counterfeit labels, 18 U.S.C. § 2318 *DMCA, 17 U.S.C. § 1201*		
Economic Espionage Act *Theft of trade secrets, 18 U.S.C. § 1831* *Economic espionage, 18 U.S.C. § 1832*	15	9.9%
Signal Piracy *Unauthorized reception of cable service, 47 U.S.C. § 553* *Unauthorized publication or use of communications, 47 U.S.C. § 605*	1	0.7%
Total	**152**	**100%**

(a)(7)(D) Department-Wide Assessment of the Resources Devoted to Enforcement of IP Crimes

The Criminal Division currently devotes 13 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 throughout FY2014 was 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 270 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 twenty 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 post a Department attorney in Bucharest, Romania.

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.

In FY 2014, the Intellectual Property Section's accomplishments included:

- The Intellectual Property Section successfully defended a challenge in the Eastern District of Louisiana to an UDRP award of the domain name "voiceofamerica.com" and further won an injunction against an individual who had been using the mark Voice of America in connection with his websites. This will help avoid both confusion of the public as to the source of these websites, which contain comments that may be viewed as offensive, and tarnishment of the Board of Broadcasting Corporation's reputation associated with its over sixty year usage of Voice of America. This case is currently on appeal to the Fifth Circuit.

- The Intellectual Property Section successfully defended a challenge to the validity of two patents covering popular table grape varieties brought in the Eastern District of California. Growers seeking to avoid paying royalties, which are used to fund research and promote California table grapes, claimed the patents were invalid. The district court sided with the government and its exclusive licensee after a three day trial. This case is currently on appeal to the Federal Circuit.

(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.