
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR

PRO IP ACT ANNUAL REPORT OF THE ATTORNEY GENERAL FY 2016

INTRODUCTION

The Department of Justice (the "Department" or "DOJ")[1] submits this Fiscal Year 2016 ("FY 2016") 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 Fiscal Year 2016 Report to Congress on Intellectual Property Enforcement ("FBI's Annual Report").

[1] Appendix A contains a glossary of acronyms referenced throughout this 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 efforts to implement them during FY 2016 (*i.e.*, October 1, 2015 through September 30, 2016) are set forth below.

In February 2010, former Attorney General Eric 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 2016 Joint Strategic Plan on Intellectual Property Enforcement, as it did with 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) <u>State and Local Law Enforcement Grants</u>

> *"(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 2016, 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, 2016, Pub. L. No. 114-113, 129 Stat. 2242, 2307, and as informed by Section 401 of the PRO IP Act. The Intellectual Property Enforcement Program ("IPEP"), as the grant program is known, is designed to provide national support and improve

the capacity of state and local criminal justice systems to address criminal IP enforcement, including prosecution, prevention, training, and technical assistance. Under the program, grant recipients establish and maintain effective collaboration and coordination between state and local law enforcement, including prosecutors, multi-jurisdictional task forces, and appropriate federal agencies, including the FBI and United States Attorneys' Offices. The information shared under the program includes information about the investigation, analysis, and prosecution of matters involving IP offenses as they relate to violations of state and local criminal statutes. The program is administered by the Bureau of Justice Assistance ("BJA"), a component of OJP.

In FY 2016, OJP was able to grant seven awards totaling $2,223,187 to local and state law enforcement and prosecutorial agencies. The following FY 2016 new awards 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
2016-ZP-BX-0001	Essex County Prosecutor's Office	$400,000
2016-ZP-BX-0002	City of Houston Police Department	$400,000
2016-ZP-BX-0003	City of Dallas Police Department	$358,534
2016-ZP-BX-0004	Louisiana Department of Justice	$150,000
2016-ZP-BX-0005	Los Angeles County Sheriff's Department	$400,000
2016-ZP-BX-0006	City of Los Angeles Police Department	$314,653
2016-ZP-BX-0007	California Department of Justice	$200,000

Since the inception of the program, OJP has awarded $24,300,209 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 law enforcement agencies have received $17,010,545. Throughout the duration of the program, these agencies have seized a total of $417,986,172 in currency and other property, which includes in counterfeit merchandise and other property valued at $411,573,202, and $6,412,966 in currency.

In addition to these seizures, grantees engaged in the following law enforcement activities in the one-year period from July 1, 2015 to June 30, 2016:

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

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

- As a result of a grant awarded in FY 2015, the Virginia State Police seized a total of $1,368,500 worth of counterfeit goods between January 2016 and June 2016.

- In FY 2016, the Los Angeles Police Department's Anti-Piracy Unit served 14 search warrants, arrested 28 individuals for IP-related crimes, and recovered evidence valued at over $10 million. In addition, the Anti-Piracy Unit provided IP investigative technique training to 690 law enforcement officers and conducted first-hand "ride-along" training to officers and prosecutors. The Anti-Piracy Unit provided training for the Beaverton Police Department, London City Police Department, Alcohol Beverage Control agents, and government delegates from the People's Republic of China ("PRC") on IP investigative techniques.

- In April 2016, the Dallas Police Department, working in conjunction with Immigration and Customs Enforcement's Homeland Security Investigations ("ICE-HSI"), the Grand Prairie Police Department, and the Dallas County District Attorney's Office, executed a search warrant on a local business, seized approximately $2.8 million worth of counterfeit goods, and arrested five individuals.

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"). Between July 1, 2015 and June 30, 2016, NW3C conducted these training sessions for 197 attendees from 106 agencies in 7 locations.[2] During this time, NW3C also conducted 2 tailored seminars for 59 attendees representing 23 agencies as well as engaged in an additional 3 technical assistance visits involving 6 agencies with 78 participants in order to improve their IP investigative and prosecutorial approaches.

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

- 89 trainings for 1,979 attendees from 1,050 agencies;
- 17 seminars for 573 attendees from 194 agencies; and
- 24 technical assistance visits for 251 attendees from 54 agencies.

[2] Training sessions took place in: Fairmont, WV; Cedar Grove, NJ; Santa Clara, CA; Jackson, MS; Raleigh, NC; Virginia Beach, VA; Portland, OR.

(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 FBI's Annual Report, 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 FBI's Annual Report, 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 2015, Congress did not appropriate funds to support Section 402(b) of the PRO IP Act in FY 2016.[3] Nevertheless, the Department has continued to take a number of actions in an effort to implement this provision. The actions, described below, include (1) increased information sharing and coordination and (2) 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 these 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 2015, 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 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 FY 2016, the Computer Crime and Intellectual Property Section ("CCIPS") of the DOJ's Criminal Division has continued to strengthen the Department's ability to combat organized IP crime through training and outreach with international counterparts and organizations, which often encounter IP crime committed by organized crime groups. These include: a November 2015 presentation on how to tackle piracy websites for a Japanese anti-piracy organization; a May 2016 training for the Mexican Attorney General's Office to assist specialized prosecutors with pending Internet piracy investigations; an August 2016 training on how to enforce IP rights overseas for American legal advisors stationed in Algeria, Bosnia & Herzegovina, Columbia, Kenya, Pakistan, Panama, and Turkey; and a September 2016 presentation to Chilean customs officials regarding IP crimes at the border.

[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."

(a)(5) Authorized Funds Under Section 403

> *"(5) With respect to the authorizations under section 403—*
>
> *(A) the number of law enforcement officers hired and the number trained;*
> *(B) the number and type of investigations and prosecutions resulting from the hiring and training of such law enforcement officers;*
> *(C) the defendants involved in any such prosecutions;*
> *(D) any penalties imposed in each such successful prosecution;*
> *(E) the advanced tools of forensic science procured to investigate, prosecute, and study computer hacking or intellectual property crimes; and*
> *(F) the number and type of investigations and prosecutions in which such tools were used."*

Section 403 related to funds appropriated during FY 2009-13. No funds were appropriated under this section or expended during FY 2016 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 in greater detail below.

Please see the FBI's Annual Report, provided separately under Section 404(c) of the PRO IP Act, for details on 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 402 and 403 of the PRO IP Act in FY 2016.

(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 in the Criminal Division, the Counterintelligence and Export Control Section ("CES") in the National Security Division, and, with regard to offenses arising under the Food, Drug, and Cosmetic Act, the Consumer Protection Branch of the Civil Division. In addition, the Department's IP Task Force, led by the Deputy Attorney General, provides high-

level support and policy guidance to the Department's overall IP enforcement efforts. Each of these components is described briefly below.

In addition to enforcing existing criminal laws protecting IP, the Department has continued its tradition of contributing to major legislative developments updating criminal IP laws, including: the Defend Trade Secrets Act of 2016, which was notable for creating a federal civil cause of action for misappropriation of trade secrets, but also increased criminal fines for organizational defendants who steal commercial trade secrets and allowed prosecutors to bring racketeering charges based on the theft of trade secrets; 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 even 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] In FY 2015, the Department also publicly supported the proposed change to the criminal copyright statute to address unauthorized online streaming as well as modification of Federal Rule of Criminal Procedure 4 to allow for simplified service of foreign corporations in trade secret theft and other cases.

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) 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 IP 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-

[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 https://www.justice.gov/iptf/pro-ip-act-reports. The Department's FY 2010-FY 2015 PRO IP Reports are available at the same location.

trained federal prosecutors who make up the Department's Computer Hacking and Intellectual Property ("CHIP") program.

CCIPS is a section within the Criminal Division consisting of a specialized team of up to forty-eight prosecutors who are devoted to enforcing laws related to computer and IP crimes. Seventeen CCIPS attorneys are assigned exclusively to IP 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 also houses the Cybercrime Lab, which provides support in evaluating digital evidence in IP cases. The Lab is currently staffed with nine computer forensics experts. In addition to evaluating digital evidence, the Lab's experts have provided extensive training on the use of digital forensics tools in IP cases to law enforcement audiences around the world.

CCIPS continues to place a high priority on fostering international cooperation and coordination of criminal IP enforcement efforts. The Section 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. Through the current program, the Department has had an experienced federal prosecutor in Bangkok, Thailand, to coordinate law enforcement activities in Asia since 2006, and, in FY 2015, the Department, working closely with the State Department, deployed a new IPLEC to Bucharest, Romania, for Eastern Europe. The IPLEC program has continued to expand in FY 2016, and with the assistance of the State Department, the DOJ has posted new regional IPLECs in Hong Kong and Sao Paolo, Brazil. In FY 2017, the State Department and DOJ expect to field a new IPLEC position in Abuja, Nigeria.

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 one or more 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.

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

The NSCS Network and CES

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 five 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 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 Counterintelligence and Export Control 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.[6] In June 2015, NSD, recognizing the increasingly acute and costly threat that economic espionage poses to the U.S. national and economic security, released its "Strategic Plan for Countering the Economic Espionage Threat." This plan aims to heighten awareness of the threat in order to deter and mitigate economic espionage. The plan also seeks to coordinate efforts within the government to counter the threat, including through operational disruption, increased and improved training, and the provision of technical advice and expertise. NSD is currently in the process of implementing the plan.

Interagency Coordination

In addition to investigating and prosecuting IP 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.[7] These activities have

[6] In 2015, CES changed its name from the "Counterespionage Section" to better reflect the scope of its work.

[7] These federal agencies include Customs and Border Protection ("CBP"), the Federal Bureau of Investigation ("FBI"), the United States Postal Inspection Service, the Food and Drug Administration's Office of Criminal Investigations, the Department of Commerce's International Trade Administration, the Naval Criminal Investigative Service, the Defense Criminal Investigative Service, the Defense Logistics Agency's Office of Inspector General, Immigration and Customs Enforcement's Homeland Security Investigations ("ICE-HSI"), the United States Nuclear Regulatory Commission, the United States Patent and Trademark Office ("USPTO"), the General Service Administration's Office of Inspector General, the Consumer Product Safety Commission, the National Aeronautics and Space Administration's Office of Inspector General, the Department of State's Office of International Intellectual Property Enforcement, the Army Criminal Investigation Command's Major Procurement Fraud Unit, the Air Force Office of Special Investigations, the U.S. Postal Service Office of Inspector General, and the Federal Maritime Commission.

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 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, seeks to support prosecutions in priority areas; promote innovation through heightened civil enforcement; achieve greater coordination among federal, state, and local law enforcement partners; and increase focus on international enforcement efforts, including reinforcing relationships with key foreign partners and U.S. industry leaders.

The IP Task Force supports the Department's efforts to aggressively investigate and prosecute a wide range of IP crimes, with a particular focus on: (1) public health and safety; (2) theft of trade secrets and economic espionage; and (3) large-scale commercial counterfeiting and piracy. The Department places a special emphasis on the investigation and prosecution of IP crimes that are committed or facilitated by cyber-enabled means or perpetrated by organized criminal networks. The IP Task Force also supports state and local law enforcement's efforts to address criminal IP enforcement by providing grants and training.

IP Task Force Members include the Assistant Attorney Generals (or equivalent) for the following components:

- Antitrust Division
- Civil Division
- Criminal Division
- Federal Bureau of Investigation
- National Security Division
- Office of Justice Programs
- Office of Legislative Affairs
- Office of Public Affairs
- United States Attorneys' Offices/Executive Office for United States Attorneys ("EOUSA")

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 2016 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 online 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 2016, this initiative resulted in a number of significant prosecutions, including those set forth below:

- *Massachusetts Man Sentenced to 37 Months in Prison for Trafficking Counterfeit Military Goods.* On October 6, 2015, Peter Picone was sentenced to 37 months in prison following his earlier guilty plea to trafficking in counterfeit military goods. From 2007 through 2012, Picone imported thousands of counterfeit integrated circuits ("ICs") from China and Hong Kong and resold them to U.S. customers, including contractors supplying ICs to the U.S. Navy for use in nuclear submarines. In addition to his prison term, Picone was ordered to pay $352,076 in restitution to the 31 companies whose ICs he counterfeited, and to forfeit $70,050 and 35,870 counterfeit ICs.

- *Indian Citizen Convicted for Selling Counterfeit Cigarettes*. On November 13, 2015, Gaurav Joseph Jayaseelan pleaded guilty to charges relating to his scheme to sell and dispense counterfeit tobacco products, the labeling of which bore the trade name of Newport

cigarettes. Jayaseelan trafficked in 53,740 cartons of cigarettes using false marks identical to and substantially indistinguishable from the registered marks of the legitimate manufacturer of Newport brand cigarettes. Undercover agents placed an order for 1,030 master cases of Newport Cigarettes for a total value of $450,625. The shipment was seized in Fort Lauderdale by Customs and Border Protection officers, in coordination with the Food and Drug Administration and U.S. Immigration and Customs Enforcement. The counterfeit cigarettes had an estimated United States street value of more than $1 million. On January 22, 2016, Jayaseelan was sentenced to 16 months in prison and one year of supervised release.

- *Former Rosemead, California Resident Sentenced to nearly Five Years in Prison for Trafficking in Counterfeit Marlboro Cigarettes*. On November 24, 2015, Su Qin Yang was sentenced to nearly five years in federal prison for trafficking in counterfeit cigarettes. Yang was also ordered to pay $308,894 in restitution to Phillip Morris USA. During the investigation, authorities seized approximately 27,500 cartons of counterfeit cigarettes and approximately $440,000 in cash. Yang pleaded guilty in May 2015 to one count of trafficking in counterfeit goods and admitted to trafficking in almost 4 million counterfeit Marlboro cigarettes and almost 4,000 counterfeit Viagra pills. Yang's husband, Antonio Limbeek, has also been charged for his involvement in the scheme and remains a fugitive.

- *Louisiana Man and His Company Sentenced for Manufacturing and Selling Counterfeit Automotive Diagnostic Equipment*. On January 14, 2016, Rainer Wittich and the company he owns, The Brinson Company ("TBC"), were sentenced for their role in creating and selling fake Mercedes-Benz diagnostic equipment containing proprietary software. Wittich was sentenced to five years of probation and ordered to pay a $3,000 fine. In addition, TBC was ordered to forfeit $150,000 and assist Mercedes-Benz in compiling a list of all customers to whom it provided the infringing devices or software. The conspirators obtained Mercedes-Benz software without authorization and manipulated the software to operate on counterfeit diagnostic devices. In total, defendants sold no less than 700 counterfeit units, with a value of over $15,000,000.

- *Pakistani Man Arrested Following Indictment for Sale and Distribution of New, Misbranded, and Counterfeit Prescription Drugs*. On January 28, 2016, Junaid Qadir was arraigned on multiple counts of illegal importation and sale of misbranded and unapproved drugs. Qadir was arrested in Germany in the spring of 2015 based on a superseding indictment that was obtained on June 25, 2015. Qadir, along with his brother and individuals known and unknown, are alleged to own and operate a business known as JNS Impex. Through JNS Impex, Qadir and his accomplices used the Internet to solicit orders for a variety of brand name and generic pharmaceutical prescriptions, mostly in commercial and wholesale quantities. Qadir and his accomplices sold primarily to individuals and entities operating Internet pharmacy websites and other types of illicit pharmacy operations who, in turn, were undertaking to sell these drugs to their retail customers without valid prescriptions. The illegal drugs included counterfeit or unapproved versions of Viagra, Lorazepam, Alprazolam, Diazepam, Zolpidem, and Phentermine. In October 2016, Qadir was sentenced to 24 months in prison and ordered to pay restitution in the amount of $17,199.

- *Rhode Island Man Sentenced for Trafficking in Counterfeit Viagra from China*. On March 31, 2016, Ricky Lugo was sentenced to a year and a day in prison and ordered to pay restitution of $104,239 for trafficking in counterfeit prescription medications. In October 2015, he was charged with four counts of trafficking in counterfeit versions of erectile dysfunction medications. From June 2013 to March 2014, Lugo sold counterfeit medications on Craigslist and in person. Lugo purchased the counterfeit pharmaceuticals from sources outside the United States, including from China.

- *Bradenton, Florida Man Sentenced To Federal Prison For Selling Counterfeit, Unapproved, and Misbranded Drugs.* On April 12, 2016, Robert Lohr was sentenced to 21 months in federal prison for his role in a conspiracy to smuggle misbranded and counterfeit drugs into the United States. He was also ordered to pay $4,276 in restitution and forfeit $926,466 as proceeds of the conspiracy. From July 2009 through September 2015, Lohr operated a business that sold and distributed illegally smuggled prescription drugs, including Viagra, Cialis, Achiphex, and Lipitor, as well as other drug products that were falsely represented as "herbal," but that contained active prescription ingredients. Lohr generated more than $1 million in sales of these misbranded and counterfeit drugs.

- *Hundreds of Counterfeit Oxycodone Tablets Seized at Port of Entry Contained Ultra-Deadly Fentanyl*. On April 14, 2016, Sergio Linyuntang Mendoza Bohon was arraigned on a charge that he unlawfully imported a controlled substance. According to a charging document, Bohon attempted to smuggle 1,183 tablets of fentanyl that were labeled as oxycodone, and 5.4 grams of powdered fentanyl. The seizure is believed to be the first time that federal officials along the California-Mexico border have intercepted counterfeit oxycodone tablets containing fentanyl as they were being smuggled from Mexico into the United States. In August 2016, Bohon was sentenced to time served and two years of supervised release.

- *Washington man sentenced to prison for importing drug paraphernalia and receipt of misbranded drugs.* On June 17, 2016, Jae Seon Yoon was sentenced to six months in prison for importing and distributing drug paraphernalia and pills that contained a variety of ingredients in dosage amounts that were never approved by the FDA and were never listed on the labels. Yoon also imported counterfeit goods, such as e-cigarettes and chargers bearing counterfeit Underwriters Laboratories markings. During the investigation, law enforcement seized enough contraband and counterfeit merchandise from Yoon's warehouse to fill nearly four extended-length semi-trucks.

- *Chinese Citizen Sentenced for Trafficking in Counterfeit Computer Chips.* On July 8, 2016, Daofu Zhang was sentenced to 15 months in prison for conspiring to sell counterfeits of sophisticated ICs to a purchaser in the United States. Zhang and his co-conspirators each operated businesses in China that bought and sold electronic components, including ICs. In the summer of 2015, they sought to purchase several advanced ICs made by Xilinx Corp. that had military applications, including radiation tolerance when used in space. Zhang's co-conspirators contacted an individual in the U.S. to procure Xilinx ICs but was informed that the desired ICs would have to be stolen from military inventory. Zhang then shipped eight counterfeit Xilinx IC's to the U.S. source to replace the ones to be stolen from the military. Zhang and his co-conspirators flew together from China to the United States in early December 2015 to meet the U.S. contact and complete the purchase. They were arrested by

law enforcement at the meeting location. One of Zhang's co-conspirators, Xianfeng Zuo, was sentenced to 15 months in prison on November 4, 2016. The other co-conspirator, Jiang Yan, was sentenced to time served on December 20, 2016.

- *Trafficker Convicted of Distributing Dangerous Counterfeit Pharmaceuticals.* On August 15, 2016, Victor Lamar Coates pleaded guilty to charges relating to a conspiracy to traffic in counterfeit Viagra and Cialis and for smuggling, trafficking, and introducing the misbranded prescription drugs into interstate commerce. Coates illegally distributed at least 10,288 counterfeit and misbranded tablets, including tablets he illegally imported directly from China. Subsequent testing on the tablets revealed that they did not contain the ingredients listed on the labeling and included compounds not part of the authentic pharmaceuticals. In December 2016, Coates was sentenced to 46 months in prison and ordered to pay $314,565 in restitution. His co-conspirator, Martez Gurley, was sentenced to 75 months in prison and ordered to pay $410,508 in restitution.

- *Las Vegas Resident Pleads Guilty in Largest-Ever Investigation of Counterfeit and Misbranded Contact Lens Operation*. On September 8, 2016, Dmitriy Melnik pleaded guilty to charges relating to his involvement in an international operation to import and sell counterfeit and misbranded contact lenses. Melnik imported thousands of colored contact lenses from the PRC and South Korea that he knew were counterfeit and/or unauthorized by the FDA for import to and sale in the United States. Melnik sold these contact lenses to tens of thousands of customers around the United States without a prescription and without adequate directions for use or adequate warnings. Melnik received at least $1.2 million in gross revenue from this illegal enterprise. Subsequent testing on some of the contact lenses sold by Melnik revealed that the lenses were contaminated with potentially hazardous bacteria. Melnik is scheduled to be sentenced in January 2017.

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

In FY 2016, 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:

- *Chinese Businessman Charged with Theft of Trade Secrets*. On October 1, 2015, Xiwen Huang was charged with one count of theft of trade secrets. From approximately December 2004 until he was fired by his employer in approximately March 2014, Huang is alleged to have stolen proprietary and confidential information, including trade secret information and other IP belonging to a government research facility and two U.S. companies, with the intent to use the stolen information for the economic benefit of himself, a Chinese company, and others. Court documents show that upon being fired in 2014, Huang returned to China with the stolen trade secrets and began working for a Chinese company in a managerial role. Huang was arrested following his return from China in May 2015 and remains in federal

custody. Huang pleaded guilty in October 2015 and was sentenced to 60 months in prison in October 2016.

- *Scientists Indicted for Allegedly Stealing Biopharmaceutical Trade Secrets*. On January 20, 2016, Yu Xue, Tao Li, Yan Mei, Tian Xue, and Luxi Xi were indicted for an alleged scheme to steal biopharmaceutical trade secrets from pharmaceutical company GlaxoSmithKline ("GSK"). Specifically, the five individuals were charged with conspiracy to steal trade secrets, conspiracy to commit wire fraud, conspiracy to commit money laundering, theft of trade secrets, and wire fraud. Yu Xue and Lucy Xi were scientists working at GSK's research facility in Upper Merion, Pennsylvania. The indictment alleges that the defendants engaged in a scheme to steal trade secrets related to GSK research data, procedures, and manufacturing processes for biopharmaceutical products. Many of the biopharmaceutical products targeted were designed to treat cancer or other serious diseases. Yu Xue, Tao Li, and Yan Mei formed a corporation in China called Renopharma allegedly to market and sell the stolen trade secret information.

- *Chinese National Pleads Guilty to Conspiring to Steal Trade Secrets.* On January 27, 2016, Mo Hailong, a PRC citizen previously employed by Beijing Dabeinong Technology Group Company ("DBN"), pleaded guilty to conspiracy to steal trade secrets. Hailong was charged in a second superseding indictment with conspiracy to steal trade secrets from several U.S.-based seed manufacturing companies, including proprietary inbred corn seeds belonging to Pioneer Hi-Bred and Monsanto, and conspiracy to transport stolen property. Five co-conspirators were charged alongside Mo, all of whom remain fugitives outside the United States and all but one of whom have ties to DBN. On October 5, 2016, Hailong was sentenced to 36 months in prison.

- *Irvine, California Engineer Named in New Indictment Alleging Theft of Trade Secrets from Two Medical Device Companies.* On May 11, 2016, a federal grand jury issued a 12-count, superseding indictment charging Wenfeng Lu with stealing and possessing trade secrets belonging to two former employers, both of which develop and manufacture medical devices used to treat cardiac and vascular ailments. During his employment, Lu travelled to the PRC multiple times—sometimes soon after allegedly downloading trade secrets from an employer's computer and emailing information to his personal email account. Lu was arrested as he prepared to board a plane to the PRC.

- *Glendale, California Man Sentenced for Stealing and Distributing Avionics Trade Secrets Belonging to Former Employer*. On June 6, 2016, Derek Wai Hung Tam Sing was sentenced to one year and one day in prison for 32 counts of violating the Economic Espionage Act. At his bench trial, the evidence showed that Sing collected trade secrets during his employment at Rogerson Kratos ("RK"), an aircraft avionics company. After he was fired, Sing retained proprietary information he had collected during his employment despite being specifically asked to return all trade secret information. Sing then prepared packages that included schematics of RK products and drafted a "readme" document explaining the importance of the proprietary information and instructing competitors to reverse engineer the products. Sing then sent the stolen trade secrets through email and physical flash drives to other companies that produced avionics, including a company outside of the United States.

- *Individual charged with Economic Espionage for Stealing Source Code from Former Employer with Intent to Benefit the Chinese Government*. On June 14, 2016, Jiaqiang Xu was charged with economic espionage and theft of trade secrets. The six-count indictment alleges that Xu stole proprietary source code from Xu's former employer with the intent to benefit the National Health and Family Planning Commission of the PRC. According to court documents, from November 2010 to May 2014, Xu worked as a developer and for this role, Xu's former employer granted Xu access to proprietary software as well as that software's underlying source code. In May 2014, Xu voluntarily resigned and subsequently communicated with undercover law enforcement officer that he had experience with his former employer's proprietary software and proprietary source code. As a result of the communications, Xu uploaded a functioning copy of the proprietary software to an undercover computer network.

- *PRC Businessman Sentenced for Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information*. On July 13, 2016, Su Bin was sentenced to 46 months in prison for his participation in a years-long conspiracy that involved Chinese military officers hacking into the computer networks of major U.S. defense contractors to steal sensitive military and export-controlled data, some of which included the companies' trade secrets, and send the stolen data to China. Su admitted that as part of the conspiracy, he sent e-mails to his co-conspirators with guidance regarding what persons, companies, and technologies to target during their computer intrusions. Once the co-conspirator stole the data through cyber intrusions, Su translated the contents of certain stolen data from English into Chinese. In addition, according to Su's admissions and the sentencing documents, Su and his co-conspirators each wrote, revised, and emailed reports addressed to the Second Department, General Staff Headquarters, Chinese People's Liberation Army about the information and technology they had acquired by their hacking activities, including its value.

- *Texas Engineer Ordered to Pay $4 Million in Restitution*. On August 19, 2016, Mattias Tezock was ordered to pay approximately $4 million in restitution for unlawfully possessing trade secrets. Tezock had previously pleaded guilty to four counts of unlawful possession of a trade secret. From April 2004 through September 2005, Tezock was employed as a chemical engineer at Voltaix, LLC. Over approximately 24 years and at great expense, Voltaix developed industry-leading trade secrets concerning the manufacture, synthesis, and purification of germane gas, a specialty chemical used in the semiconductor and solar energy industries. When Tezock was terminated from employment with Voltaix, he established Metaloid Precursors, Inc., and began misappropriating Voltaix's confidential, proprietary, and trade secret recipe and process for manufacturing and purifying germane gas. Tezock additionally solicited business from Voltaix's customers.

(3) Large-Scale Commercial Counterfeiting and Online Piracy

The Department continues to pursue significant, large-scale piracy and counterfeiting operations. In FY 2016, the Department has had a number of significant prosecutions, including those set forth below:

- *Husband and Wife Charged with Conspiring to Traffic Millions of Dollars' Worth of Counterfeit Goods.* On October 15, 2015, Le Fu Chen and Hai Fan Huang were charged for their role in a conspiracy to traffic in counterfeit goods. Between November 2014 and October 2015, Chen and Huang are alleged to have imported counterfeit luxury and designer brand goods into the United States from China. During the investigation, law enforcement agents conducted searches of Chen and Huang's storage units, business suites, and residence, and seized over 130,000 pieces of luxury and designer brand counterfeit goods worth millions of dollars. In October 2016, Chen and Huang each pleaded guilty to conspiring to traffic in counterfeit goods. Also in October 2016, Chen was sentenced to 24 months in prison, and Huang was sentenced to one year of probation. Both defendants were ordered to pay $2,961,428 in restitution.

- *Operator of Second-Largest Music Piracy Cyberlocker in United States Sentenced to 36 Months in Prison for Criminal Copyright Infringement.* On November 17, 2015, Rocky Ouprasith was sentenced to 36 months in prison and two years of supervised release based on his conviction for criminal copyright infringement. He was also ordered to forfeit $50,851.05 and pay $48,288.62 in restitution. Between May 2011 and October 2014, Ouprasith operated RockDizMusic.com, a website where Internet users could find and download infringing digital copies of popular, copyrighted songs and albums. Ouprasith admitted that he obtained digital copies of copyrighted songs and albums—including "pre-release" songs that were not yet commercially available to consumers—from online sources and solicited others to upload digital copies of copyrighted music as well. According to the Recording Industry Association of America, in 2013, RockDizFile.com was the second-largest online file-sharing website specializing in the reproduction and distribution of infringing copies of copyrighted music in the United States. According to court documents, the market value of Ouprasith's illegally-pirated material was more than $6 million.

- *Operation Software Slashers: Sixth Defendant Pleads Guilty to $100 Million Software Piracy Scheme.* On December 16, 2015, Rex Yang, Jr. pleaded guilty to a federal information that charged him with participating in a criminal conspiracy from January 2009 to December 2014. Yang, who owned and operated Digisoft LLC and Premiere Software Inc., is the sixth and final defendant to plead guilty in separate, but related, cases in this ongoing criminal investigation. The multimillion-dollar scheme, which involved co-conspirators operating in the PRC, Singapore, Germany, and the United States, illegally sold more than 170,000 product activation codes for Microsoft Corp. and Adobe Systems Inc. software. Investigators seized more than $20.6 million in assets through federal forfeitures, including $10,188,777 from bank and investment accounts, 10 luxury automobiles, and 27 parcels of real estate. Affidavits filed in those forfeiture complaints estimate that conspirators reaped about $30 million in profits from customers who paid more than $100 million for the software. Yang is scheduled to be sentenced in June 2017.

- *New Orleans Man Sentenced to 41 Months for Manufacturing and Selling More Than $1 Million in Counterfeit Coupons on Silk Road.* On January 13, 2016, Beau Wattigney was sentenced to 41 months in prison for his role in a coupon counterfeit ring using the Silk Road marketplace, a covert online marketplace largely for illicit goods. Wattigney previously pleaded guilty to conspiracy to commit wire fraud and conspiracy to commit trademark

counterfeiting. According to the plea agreement, Wattigney sold over $1 million worth of counterfeit coupons and victimized more than 50 businesses based in the United States.

- *Conspirators in Two Android Mobile Device App Piracy Groups Plead Guilty*. On January 13, 2016, Gary Edwin Sharp II pleaded guilty to one count of conspiracy to commit criminal copyright infringement for his role in a scheme to distribute more than four million pirated copies of copyrighted Android apps with a total retail value of more than $17 million. Then, on May 2, 2016, his co-conspirator, Aaron Blake Buckley, pleaded guilty to one count of conspiracy to commit criminal copyright infringement and to one count of criminal copyright infringement for his role in the scheme. The conspirators were members of the Applanet Group. From May 2010 through August 2012, they conspired to reproduce and distribute more than four million copies of copyrighted Android apps through the Applanet alternative online market without permission from the victim copyright owners, who would otherwise sell copies of the apps on legitimate online markets for a fee. Buckley is scheduled to be sentenced in January 2017, and Sharp is scheduled to be sentenced in February 2017.

- *Brothers Sentenced for $12.9 Million Software Piracy Scheme.* On April 7, 2016, Deonnetti Deantoni was sentenced to forty months in prison, $6.5 million in forfeiture, and $7.7 million in restitution for his role in a large scale software piracy scheme. His brother, Donnetto Deantoni, was sentenced on August 10, 2016, to one year and a day in prison, $4.4 million in forfeiture, and $12.9 million in restitution for his role in the scheme. Over the course of 26 months, the brothers conspired to distribute pirated versions of nearly $13 million worth of copyrighted engineering and design software belonging to Autodesk, Inc. The brothers sold this software to engineering firms at deeply discounted prices using websites designed to make the software appear legitimate and went to great lengths to conceal their scheme.

- *Missouri Woman Pleads Guilty to $80 Million Fraud Scheme to Sell Counterfeit Cell Phone Parts.* On May 26, 2016, Sherrie Householder pleaded guilty to an information charging her with one count of mail fraud, one count of money laundering, and one count of tax evasion. Householder admitted that she received more than $80 million from the sale of counterfeit items over approximately three years. Householder managed and operated Flash Technology, LLC, a business that sold cell phone components over the Internet and at a physical storefront. These counterfeit components bore trademarks that made them appear legitimate, and Householder used the trademarks and logos of these companies on her websites. Wang "Frank" Lou, a Chinese citizen, owned Flash Technology, while Householder managed the company's activities in the United States. Nearly 5,000 international shipments were sent to Flash Tech from China. Law enforcement seized approximately $5.5 million worth of counterfeit cell phones, electronics, and component parts from Householder's residence and at the storefront. Householder's sentencing is scheduled for January 2017.

- *Chinese National Indicted for Software Piracy Scheme*. On June 29, 2016, Wen Tao Liu was charged with conspiracy, trafficking in counterfeit goods, smuggling goods into the United States, and entry of goods by means of false statements. Liu allegedly obtained and sold counterfeit, illicit, and/or unauthorized Microsoft software, software products and related components, including unauthorized product key codes and counterfeit product key cards, costing the Microsoft Corporation millions of dollars in losses. Investigators identified at least 4,659 individual product activation key codes distributed by Liu to various resellers

across the United States, which were collectively activated over 36,000 times. Microsoft had already blocked 1,111 of those keys due to suspicions of piracy and 2,267 of the keys were already identified in the course of other Microsoft fraud investigations. Microsoft's losses from the repeated activations of the 4,659 product keys total approximately $9 million.

- *Owner of Most-Visited Illegal File-Sharing Website Charged with Copyright Infringement*. On July 20, 2016, Artem Vaulin was charged with one count of conspiracy to commit criminal copyright infringement, one count of conspiracy to commit money laundering, and two counts of criminal copyright infringement. Vaulin is the alleged owner of Kickass Torrents, the most visited illegal file-sharing website which has allowed users to illegally reproduce and distribute hundreds of millions of copyrighted motion pictures, video games, television programs, musical recordings, and other electronic media since 2008. The copyrighted material is collectively valued at well over $1 billion, according to court documents. Law enforcement has seized domain names associated with the website and is seeking to extradite Vaulin to the United States from Poland, where he was arrested.

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 among federal, state, and local law enforcement agencies. Examples of such training included:

- In October 2015, NSD, with support from CCIPS, organized and led the annual NSCS Training in Mclean, Virginia. 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. 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 issues related to the investigation, prosecution, and disruption of crimes impacting national security.

- In December 2015, CCIPS organized and taught its Intellectual Property Seminar at the National Advocacy Center ("NAC"). The Seminar featured an in-depth course on investigating and prosecuting the trafficking of counterfeit goods and services, criminal copyright, and theft of trade secrets, along with significant instruction on electronic evidence gathering for IP cases.

- In March 2016, CCIPS hosted its annual CHIP Conference and Training at the NAC. Approximately 150 prosecutors attended the four-day event, which featured training on a wide range of investigative, litigation, legislative, and technology issues. The conference also included multiple breakout sessions, and an optional day with two tracks—a refresher track, and an advanced technology track.

- In April 2016, CCIPS presented at the Hanscom Air Force Base in Massachusetts on the investigation and prosecution of cases involving trafficking in counterfeit microelectronics.

The audience consisted of 50 members of the Boston Area Fraud Working Group, which includes procurement and auditing personnel from the Air Force and other government agencies, as well as members of federal and local law enforcement. CCIPS also provided a more tailored presentation to 12 attorneys and staff at the base.

- In April 2016, CCIPS presented a case study to ICE-HSI agents at the IPR Center in Virginia. The case study focused on *United States v. Ouprasith*, which involved a defendant who was convicted of criminal copyright infringement for his role in operating what the industry described as the second largest infringing music cyberlocker in the country. Ouprasith is the first cyberlocker operator to be convicted and sentenced for criminal copyright infringement.

- In May 2016, CCIPS presented to 40 investigative agents and procurement personnel at the Department of Defense Washington Headquarters in Virginia. The presentation focused on *United States v. Picone* and the prosecution of those who traffic in counterfeit integrated circuits.

- In May 2016, CCIPS organized and taught the Electronic Evidence and Basic Cybercrime Seminar at the NAC. The seminar, which was attended by approximately 70 prosecutors, addressed a variety of topics including: obtaining evidence from third-party service providers pursuant to the Stored Communications Act, the Pen/Trap Statute, and the Wiretap Act; the utility of social networking sites to investigations; the search and seizure of electronic media; encryption; basic principles relating to the Internet; digital forensics; the use of electronic evidence at trial; and relevant statutes governing computer and IP crime.

- In June and August 2016, CCIPS gave two presentations at the Intellectual Property and Trade Enforcement Investigations Courses hosted at the Federal Law Enforcement Training Center in Glynco, Georgia. The presentations, which were attended by approximately 50 ICE-HSI and CBP agents, covered the relevant law and policy surrounding IP prosecutions, as well as practical guidance in counterfeit trademark investigations.

- Throughout FY 2016, CCIPS provided eight trainings across the United States to agents involved in Operation Chain Reaction, an ongoing law enforcement effort to target counterfeit and substandard parts in the military supply chain. These agents hailed from offices in Los Angeles, California; Washington, DC; Atlanta, Georgia; Miami, Florida; San Juan, Puerto Rico; Newark, New Jersey; Buffalo, New York; Chicago, Illinois; Detroit, Michigan; Phoenix, Arizona; El Paso, Texas; New Orleans, Louisiana; Dallas, Texas; Houston, Texas; and San Antonio, Texas. The presentations focused on how to effectively prosecute traffickers in counterfeit integrated circuits and featured a case study of *United States v. Picone*, which involved a defendant convicted of selling counterfeit integrated circuits to the U.S. Navy for use in nuclear submarines.

International Outreach and Training

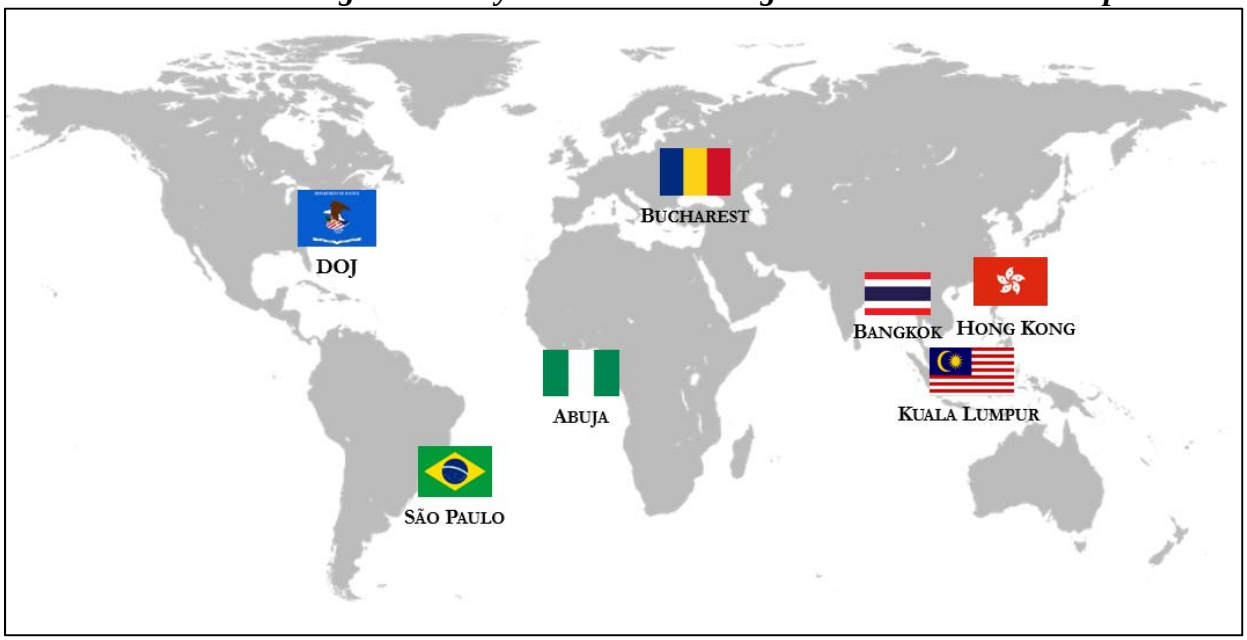
Global IP crime, from the manufacture and worldwide distribution of counterfeit goods, to the sprawling online businesses designed to reap profits from the distribution of copyrighted works, continues to grow and change in an effort to stay ahead of law enforcement. As a world

leader in efforts to combat criminal IP infringement, the Department actively seeks to develop training and technical assistance programs to assist other countries in effectively enforcing IP laws and reducing the trafficking of counterfeit and pirated goods. Despite budgetary constraints, in FY 2016 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 2016 to provide training to foreign officials on effective enforcement of IP laws. CCIPS's IP trainings are designed to increase cooperation between various law enforcement agencies with responsibility for IP offenses; to utilize various types of charges, including economic and organized crime statutes to combat IP crime; and to increase awareness amongst enforcement officials and the judiciary of the importance of reducing counterfeiting and piracy.

In FY 2016, an experienced CHIP Attorney continued his service as the third IPLEC in Bangkok, Thailand. Another experienced CHIP attorney continued service in Bucharest, Romania, as the Eastern Europe IPLEC. The Department, with the assistance from the State Department, expanded the IPLEC program by posting new regional IPLECs in Hong Kong and Sao Paolo, Brazil. The program is expected to continue expanding in FY 2017 with a new position in Abuja, Nigeria.[8]

DOJ's IPLEC Program and Cyber Intermittent Legal Advisor in Kuala Lumpur



[8] For more information about CCIPS's international outreach, see https://www.justice.gov/criminal-ccips/overseas-work.

In addition to the Department's regional efforts through its IPLEC program, examples of DOJ's international engagement regarding various IP enforcement include:

CHINA

U.S.-China Joint Liaison Group on Law Enforcement Cooperation. The Department continues to engage with China through the bilateral IP Criminal Enforcement Working Group ("IPCEWG"), which is part of the Joint Liaison Group ("JLG"). The JLG is designed to strengthen law enforcement cooperation between the United States and China across a range of issues, including IP and cybercrime. In November 2015, CCIPS participated in the 13th Annual Meeting of the JLG in Washington, D.C. Deputy Assistant Attorney General Bruce Swartz co-chaired the JLG plenary session. Also in attendance at the JLG meeting were representatives from DOJ, DOS, FBI, ICE-HSI, and DEA. In March 2016, CCIPS also participated in the IPCEWG's annual meeting in Washington D.C., and discussed the continued commitment to ongoing case cooperation and coordination, joint priority areas, and proposals for the upcoming year.

U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues. In December 2015, Attorney General Loretta E. Lynch and Department of Homeland Security Secretary Jeh Johnson, together with Chinese State Councilor Guo Shengkun, co-chaired the first U.S.-China Joint Dialogue on Cybercrime and Related Issues. Under the commitments made by U.S. President Barack Obama and Chinese President Xi Jinping during the state visit in September 2015, the primary objectives of the dialogue were to review the timeliness and quality of responses to requests for information and assistance with respect to cybercrime or other malicious cyber activities and to enhance cooperation between the United States and China on cybercrime and related issues. In addition to members of the Departments of Justice and Homeland Security, representatives from the Department of State, National Security Council and Intelligence Community participated for the United States, while the Chinese delegation included representatives from the Committee of Political and Legal Affairs of CPC Central Committee, the Ministry of Public Security, the Ministry of Foreign Affairs, the Ministry of Industry and Information Technology, the Ministry of State Security, the Ministry of Justice and the State Internet Information Office. During the dialogue, both countries discussed ways to enhance cooperation within the bounds of each nation's legal framework and assessed progress made on cases identified during their discussions in September 2015. The December 2015 meeting resulted in a decision to, among other things, further develop case cooperation on cyber-enabled crimes, including the theft of trade secrets. The second U.S.-China Joint Dialogue on Cybercrime and Related Issues took place in June 2016 and resulted in a commitment to prioritize cooperation on combatting cyber-enabled IP theft for commercial gain.

U.S.-China Legal Exchange on Cross-Border Enforcement of IP Rights. In March 2016, CCIPS participated in a panel discussion entitled "Cross-border Enforcement of IPR in the Internet Environment" alongside representatives from Chinese law enforcement and private industry. The panel discussion was part of a day-long U.S. Department of Commerce-sponsored program at the USPTO's Global Intellectual Property Academy covering U.S.-China interaction on IP issues. Approximately 130 government and industry representatives attended.

Training with Ministry of Public Security. In June 2016, the IPLEC based in Hong Kong conducted a training in Shenzhen, China, for approximately 150 officers with the Ministry of Public Security, Economic Crime Investigation Department, on asset forfeiture in IP cases. The training, conducted jointly with the U.S. DOJ Resident Legal Advisor for Beijing, also included blocks on drafting Mutual Legal Assistance Agreement requests and legal process for tracking fugitives.

Meetings with Chinese Government Delegations. During FY 2016, CCIPS met with a number of visiting Chinese government officials to discuss U.S. criminal enforcement of IP rights. These meetings included: a November 2015 presentation to 16 members from the IP Bureau of Hunan Province organized by the University of Maryland's Office of International and Executive Programs; an April 2016 meeting with Chinese judges organized by USPTO's Office of Policy and International Affairs; and a July 2016 meeting with Chinese judges and lawyers organized by the U.S. State Department's International Visitor Leadership Program.

NORTH AFRICA AND THE MIDDLE EAST

International Training on IP Criminal Enforcement. In November 2015, CCIPS participated in a USPTO-sponsored training on IP criminal enforcement in Rabat, Morocco, for approximately 50 police and investigators from Morocco, Cameroon, Senegal, and the Ivory Coast. The presentation focused on the investigation and prosecution of trademark counterfeiting, copyright infringement, theft of trade secrets, counterfeit labels, bootlegging, camcording, and Digital Millennium Copyright Act ("DMCA") violations.

State Department Bilateral Training in Nigeria. In August 2016, CCIPS participated in a cyber-oriented training for Nigerian judges and legislators organized by the State Department's Office of the Coordinator for Cyber Issues. CCIPS provided a significant portion of the instruction during the four-day workshop and presented on topics including cybercrime offenses, IP offenses, mutual legal assistance, the Budapest Convention, cell-phone based evidence, methods of identifying a perpetrator of an Internet-enabled crime, and the use of electronic evidence at trial.

IP Training Event for African Investigators: In August 2016, CCIPS presented on International Cooperation at a training event hosted by the IPR Center and ICE-HSI at the Marshall Center in Garmisch-Partenkirchen, Germany. Approximately 40 participants hailed from investigative agencies in Togo, Morocco, Senegal, Nigeria, and the Ivory Coast.

Training for Middle East/North African Prosecutors and Investigators. In September 2016, CCIPS and the Cybercrime Lab trained approximately 35 prosecutors and investigators at the "Regional Workshop on Investigating and Prosecuting Intellectual Property Violations" in Amman, Jordan. The workshop, designed to help prosecutors and investigators develop a regional network of IP enforcement authorities and foster bilateral and regional cooperation, was sponsored by OPDAT and CCIPS. Prosecutors and criminal investigators from Egypt, Jordan, Lebanon, Morocco, and Saudi Arabia attended the workshop. CCIPS provided training regarding the development of leads, working with rights holders, evidentiary issues, and charging decisions in both counterfeit pharmaceuticals and Internet-based IP crime investigations. CCIPS also led a

multi-day interactive question-and-answer discussion of three detailed hypothetical case studies, including how each country's representatives would address different IP investigation and case issues, followed by actual case studies. The Cybercrime Lab trained investigators on how to use publicly available computer forensic tools, techniques for detecting and circumventing encryption, as well as securing and obtaining evidentiary copies of digital evidence from computer systems. United States District Judge Richard Stearns, along with attorneys and analysts from the DOJ, concluded with a mock sentencing demonstration.

CENTRAL AND SOUTH AMERICA

Meeting with Mexican PGR's Digital IP Crime Unit. In November 2015, CCIPS and the Cybercrime Lab met with the Deputy Attorney General for Federal Crimes from Mexico's Procuraduría General de la República ("PGR") (Office of the General Prosecutor), the Director of PGR's Specialized IP Unit, and prosecutors from PGR's new digital IP Crime unit. PGR recently created the IP Crime Unit to focus on the investigation and prosecution of cyber-enabled IP crimes. At the meeting, CCIPS discussed the challenges that arise in the investigation and prosecution of digital IP crimes, opportunities for future joint training, and hardware and software requirements for digital forensic analysis.

Meeting with Brazilian Delegation. In November 2015, CCIPS met with a visiting delegation of Brazilian investigators, police, and customs officials to discuss common IP criminal enforcement issues. The delegation included leaders of anti-piracy squads at several regional civil police departments, a senior financial crimes investigator, customs supervisors from the largest express consignment facility and the largest port in Brazil, and the director of the federal highway police. The ICE-HSI Attaché in Brasilia, who has been coordinating joint IP law enforcement efforts by ICE-HSI and Brazilian law enforcement, accompanied the delegation.

Video Conference with Mexican Prosecutors. In May 2016, CCIPS and the Cybercrime Lab conducted a digital video conference in Washington, D.C., with the Mexican Attorney General's Office to assist specialized Mexican prosecutors with pending Internet piracy investigations. Following up on training conducted for Mexican law enforcement last year by CCIPS and others on IP rights enforcement issues, the Mexican government created a new digital piracy IP unit staffed by four prosecutors and is now actively investigating several illicit sites.

Presentation to Chilean Law Enforcement. In September 2016, CCIPS presented at the USPTO's Global Intellectual Property Academy in Alexandria, Virginia, regarding combating IP crimes at the border. Approximately 20 customs officers and other Chilean officials attended the conference.

EUROPE

Meeting with Members of the European Parliament. In November 2015, CCIPS attended a meeting hosted by the IPEC with seven members of the European Parliament to discuss challenges in enforcing IP rights. Representatives from CBP, DHS, and ICE-HSI also attended. The meeting focused on U.S. efforts to disrupt large-scale Internet piracy operations and the growth of counterfeit goods trafficking. The discussion also covered existing challenges to

cooperative, international law enforcement efforts rooted in different legal regimes and the speed and flexibility across international borders of modern IP infringers.

Eastern Europe IPLEC and CCIPS Train on Combatting Online Piracy. In November 2015, the Eastern Europe IPLEC coordinated a two-day training session on investigating and prosecuting cases of online piracy. Moldova, Bulgaria, and Turkey each sent a delegation of five law enforcement officers and prosecutors, and Romania's delegation included approximately two dozen investigators and prosecutors. The program provided participants with a current view of legal issues surrounding the investigation and prosecution of online piracy, including updates on data retention legislation.

IPLEC Travels with Eastern European Delegation through United States. In January 2016, the Eastern Europe IPLEC traveled with a delegation from Eastern Europe to Washington, D.C., San Francisco, and the Silicon Valley. The delegation included 13 investigators, prosecutors, and judges from Romania, Bulgaria, Moldova, Hungary, and Poland. The visit was designed to highlight how the United States approaches the criminal enforcement of IP rights. The delegation had several productive meetings in Washington, D.C., with the State Department's Bureau of International Narcotics and Law Enforcement and Office of International IP Enforcement, the USPTO's Office of Policy and International Affairs, and ICE-HSI. During the California phase of the program, the delegation met with Judge Margaret McKeown, a staff attorney at the Ninth Circuit Court of Appeals, and federal and state prosecutors.

Meeting with French Officials. In February 2016, CCIPS met with two representatives of the French government who are involved in investigating and prosecuting terrorism crimes. The meeting covered CCIPS's role in the Department's strategy to combat cybercrime and IP crimes, as well as current issues related to encryption and the collection of electronic evidence.

Presentation at the EU's Intellectual Property Prosecutor's Network. In March 2016, CCIPS presented a case study on business models used to commit IP crimes online to IP prosecutors from 21 EU countries and 6 non-EU European countries. The case studies featured examples of prosecutions in which the EU and the United States have worked together to successfully combat online IP crime. The EU IP prosecutors are part of the EU's newly established "European Intellectual Property Prosecutor's Network," and the workshop was held in Alicante, Spain. This was the first time that the Network has met since it was created in 2015. The Eastern Europe IPLEC also attended the workshop.

IP Enforcement Training for Southeast European Investigators. In June 2016, CCIPS presented on the subject of international cooperation and information sharing in IP investigations during a training program on Intellectual Property Enforcement for criminal investigators from several southeast European countries. The three-day program, organized by ICE-HSI and the National IPR Center, was conducted at the International Law Enforcement Academy in Budapest, Hungary. The program provided training for approximately 30 investigators from Ukraine, Romania, Serbia, Albania, and Montenegro on criminal IP enforcement and related issues, including online investigative techniques, virtual currencies, and money laundering.

Training on Digital Evidence and Forensic Analysis at the Hungarian Judicial Academy. In August 2016, the Cybercrime Lab presented at a conference organized by the IPLEC in Budapest, Hungary, on Internet-facilitated IP crimes. The presentations included an overview of digital evidence and computer storage methods as well as a hands-on workshop in computer forensics. Approximately 60 participants from across Europe attended, including law enforcement officers, prosecutors, judges, and industry representatives.

Presentation at Interpol IP Crime Conference. In September 2016, CCIPS participated in and gave a plenary presentation at INTERPOL's 2016 International Law Enforcement IP Crime Conference held in London. The conference is an international law enforcement/industry conference co-hosted this year by INTERPOL and the City of London Police, in partnership with Underwriter's Laboratories. The conference brought together over 600 law enforcement and customs personnel from 70 countries to gain an international perspective on the trade in counterfeit and pirated products, to share international best practices on how to combat this illegal trade effectively, and to provide a global forum for networking and partnership development.

OTHER REGIONS

Training South Asian Officials and Attorneys on Intellectual Property Enforcement. In October 2015, CCIPS presented an overview of U.S. criminal IP enforcement to a delegation from India, Pakistan, and Bangladesh that included government officials, law professors, and representatives of the music, pharmaceutical, and agricultural sectors. Topics included investigation and prosecution of trademark counterfeiting and copyright piracy cases, as well as international cooperation in IP enforcement. The group was visiting the United States as part of the State Department's International Visitor Leadership Program and also met with representatives of FBI and the Department of Commerce.

Meeting with Japanese Anti-piracy Organization. In November 2015, CCIPS met with executives from the Tokyo-based Content Overseas Distribution Association ("CODA") at the IPR Center in Arlington, Virginia. CODA seeks to protect against infringement of Japanese copyrighted works around the world and sought advice on how to deal with various Chinese-run pirate sites distributing Japanese movies, TV shows, anime, manga, and other copyrighted works over the Internet without permission.

Presentation to Taiwanese Prosecutors and Investigators. In December 2015, CCIPS presented to Taiwanese prosecutors and investigators on investigating and prosecuting trade secret theft cases. The presentation, given over digital video conference, included a nuts-and-bolts discussion of how prosecutors prove the existence of a trade secret in U.S. cases, how we prepare search warrants in IP crime cases, and how we collect digital evidence in IP crime cases. The audience included 41 prosecutors and investigators from Taiwan's Ministry of Justice's Department of Prosecutorial Affairs, the Intellectual Property Branch of Taiwan's High Prosecutor's Office, and various District Prosecutor's Offices.

Address to Indian Officials on Criminal Copyright Enforcement. In April 2016, CCIPS presented an overview of criminal copyright enforcement and emerging issues in online enforcement as

part of a two-day copyright seminar for Indian government officials. The program took place at the Global Intellectual Property Academy at the U.S. Patent and Trademark Office in Alexandria, Virginia.

Presentation at the International Law Institute. In June 2016, CCIPS gave two presentations to foreign judges and law enforcement officials at the International Law Institute in Washington, D.C. The presentations focused on investigating and prosecuting cybercrime and IP crime.

Panel Discussion at the International Copyright Institute: In June 2016, CCIPS took part in a panel presentation at the Copyright Office's International Copyright Institute. The panel included the Director of the National IPR Center and an FBI Intelligence Analyst, and focused on coordination among prosecutors and investigators in identifying and prosecuting IP cases. The audience consisted of copyright officials from 19 countries.

CCIPS Hosts Intellectual Property Delegation from Thailand. In June 2016, CCIPS hosted a delegation of 11 prosecutors and law enforcement officers from Thailand as part of a workshop sponsored by the USPTO's Global Intellectual Property Academy. CCIPS and the Cybercrime Lab presented on various topics relating to IP, including working with victims, electronic evidence, forensics, and prosecution strategies.

Training at DOJ/OPDAT Resident Legal Advisor School. In August 2016, CCIPS addressed 11 participants based in seven countries—Algeria, Bosnia & Herzegovina, Columbia, Kenya, Pakistan, Panama, and Turkey—at the DOJ/OPDAT Resident Legal Advisor School in Washington, D.C. The presentation focused on cybercrime and electronic evidence issues, and CCIPS's role in providing technical legal advice and assistance. CCIPS also discussed DOJ's work on IP matters, the IPLEC program, how to work on IP rights enforcement overseas, and recurring general IP issues in U.S. embassies around the world.

Presentation at WIPO–U.S. Intellectual Property Rights Event. In August 2016, CCIPS presented at a two-week workshop organized by the World Intellectual Property Organization in cooperation with the USPTO. The event took place in Alexandria, Virginia, and also featured speakers from FBI and CBP. In attendance were private-sector individuals from the design industries of Bangladesh, Brazil, Canada, Finland, Gambia, India, Italy, Korea, Pakistan, Peru, Saudi Arabia, and South Africa.

Presentation for Visiting Judges from Pakistan. In August 2016, CCIPS presented on the prosecution of IP crime as part of a "Judicial Exchange on the Protection of Intellectual Property Rights" with visiting judges from Pakistan. The presentation also included topics pertinent to sentencing and asset forfeiture, and CCIPS designed and participated in a sentencing hearing demonstration with U.S. District Judge Leonie M. Brinkema. The USPTO, the U.S. Embassy in Pakistan, and the Intellectual Property Organization of Pakistan sponsored the program.

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, in September 2016, CCIPS hosted the tenth annual IP Industry and Law Enforcement Meeting 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. This year, Assistant Attorney General Leslie Caldwell provided introductory remarks, and several senior DOJ and law enforcement officials, including U.S. Attorney for the District of Maryland Rod Rosenstein and officials from FBI, ICE-HSI, CBP, and FDA participated in the meeting. Approximately 90 industry representatives 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: the Annual Meeting of the Defense Research Institute in October 2015; Practising Law Institute's Conference on Intellectual Property Rights Enforcement in January 2016; the Global Innovation Strategy Seminar at Georgetown University in April 2016; the ABA's Section of International Law Spring Meeting in April 2016; a meeting with the IP Section of the California Bar Association in April 2016; a meeting with Global Brand Protection at Cisco Systems, Inc. in April 2016; the Symposium on Counterfeit Parts and Materials organized by the Surface Mount Technology Association and the Center for Advanced Life Cycle Engineering in June 2016; the Seattle Export Controls Conference in July 2016; and the Copyright Seminar sponsored by USPTO's Global Intellectual Property Academy in September 2016.

In addition, other select Department outreach to industry groups affected by IP crime included:

- On November 4, 2015, CCIPS attorneys met with representatives from Eli Lilly, Boehringer Ingelheim, the Alliance for Safe Online Pharmacies, and IPR Center partner agency representatives to discuss U.S. government activities related to Internet pharmacies, how to increase information sharing and collaboration between industry and law enforcement, and public awareness opportunities.

- On November 10, 2015, and February 3, 2016, CCIPS met with representatives of the Entertainment Software Association, Business Software Association, Recording Industry Association of America, and Motion Picture Association of America to discuss how rights-holders may best initiate a federal criminal investigation of IP crimes and support criminal prosecutions of such crimes.

- On December 8, 2015, CCIPS Attorneys, as well as FBI and ICE-HSI representatives, met with Internet researchers from RiskIQ and representatives from Digital Citizens Alliance and NBC Universal to discuss the connections between content theft sites and malware distributions.

- On February 2, 2016, CCIPS presented at the Cyber Initiative and Roundtable at Louisiana State University to over 70 individuals from the business and law enforcement community to discuss efforts to report and combat cybercrime and theft of trade secrets.

- On February 12, 2016, CCIPS and the FBI participated in a roundtable meeting with local companies to discuss how law enforcement approaches cyber investigations and how cyber intrusions or trade secret theft can be reported. The roundtable also covered the legal issues facing private sector companies, including issues arising under the newly enacted Cybersecurity Act of 2015.

- On February 18, 2016, CCIPS participated in a panel discussion at Fordham Law School to general counsels from 35 different New York companies and discussed how to report cyber intrusions or trade secret theft, as well as legal issues associated with information sharing, including issues arising under the Cybersecurity Act of 2015.

- On February 18, 2016, and September 29, 2016, CCIPS and the IPR Center co-hosted a half-day meeting of the Counterfeit Microelectronics Working Group, which meets at least twice a year to discuss ways to detect and prevent counterfeit microelectronics in the U.S. supply chain. In total, approximately 120 representatives from law enforcement, other government sectors, and private industry attended the meeting.

- On March 10, 2016, CCIPS presented to approximately 250 government, industry, and private sector representatives at the 22nd Annual Federal Procurement Institute on the federal criminal response to counterfeit goods, including what to expect in a criminal investigation and prosecution.

- On March 10, 2016, CCIPS participated in meetings with representatives of the Automotive Anti-Counterfeiting Council ("A2C2"). The IPEC, IPR Director at CBP, and DOJ Office of the Deputy Attorney General participated in a closed morning session with IPR Center partners, CCIPS, and A2C2 representatives. The afternoon symposium consisted of A2C2 and FBI briefings and an open discussion regarding numerous topics, including emerging threats and challenges, key indicators for law enforcement, supply chain and packaging indicators, communication methods and social media, express consignment carriers, and payment systems.

- On March 29, 2016, CCIPS participated in a panel discussing the misappropriation of commercial trade secrets to audiences at Iowa State University in Ames (focusing on agriculture and related industries) and at Drake University in Des Moines (focusing on financial sector businesses). Other participants in the panel included a local Assistant U.S. Attorney ("AUSA") and representatives of the FBI Counterintelligence Division and

NSD. The panel discussions at each event followed keynote remarks from the Assistant Attorney General at NSD and the Deputy Assistant Director of the FBI's Cyber Division.

- On June 1, 2016, CCIPS participated in a half-day roundtable at the U.S. International Trade Commission ("USITC") on trade secrets. The roundtable consisted of 25 government officials, industry representatives and executives, academics, and others dealing with the protection of trade secrets, and was led by all six USITC commissioners.

- On June 14, 2016, CCIPS spoke at a law enforcement roundtable hosted by the Entertainment Software Association in Los Angeles, California. The roundtable included representatives from state law enforcement and industry, and was part of the annual E3 Exposition. CCIPS discussed the need for increased public-private cooperation and best practices for building an IP crime case.

- On September 28, 2016, CCIPS gave two presentations to approximately 40 IP industry representatives and private sector attorneys at the Anti-Counterfeiting & Brand Protection Summit in Arlington, Virginia. The first presentation was co-presented with the National Cyber Forensics & Training Alliance and focused on combatting trademark counterfeiting activity on the Internet. The second covered how to reduce online counterfeiting rings overseas and was co-presented with the U.S. Chamber of Commerce.

NSD has undertaken strategic changes within its Division designed to put additional focus on the protection of national assets from the threats of nation states, including economic espionage and trade secret theft. These changes included creating a new Deputy Assistant Attorney General position focusing on protecting national assets and naming the first Director of the Division's Protection of National Assets Outreach Program. Pursuant to this increased focus, NSD leadership and other attorneys have reached out to senior managers and counsel at hundreds of companies over the last year to educate them about the Department's resources and efforts to combat economic espionage and trade secret theft and other national security threats. These outreach efforts have included presentations at universities and think tanks, cybersecurity summits and roundtable discussions, as well as one-on-one meetings with senior executives at Fortune 500 and other companies. The NSCS Network also periodically disseminated talking points and other resources to its members nationwide to facilitate their outreach to companies and other organizations in their home districts and facilitated FBI field offices' efforts to educate AUSAs on the national security threats in their districts and to include them in FBI's outreach efforts in their districts.

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 https://www.justice.gov/iptf and https://www.cybercrime.gov. The National IPR Center also has a website where the public can report IP theft. That site can be found at https://www.iprcenter.gov.

The award that funded the IP Public Education Campaign ended in FY 2015. The campaign, which launched in November 2011, aimed to raise the public's awareness of the impact of counterfeit and pirated products, change the widely-accepted belief that purchasing counterfeit and pirated products is not harmful, and reduce demand for counterfeit or pirated products by influencing the behaviors of at-risk consumers. The content generated as part of this campaign remains available on the BJA website.[9]

(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 2016, listing the number of defendants and cases charged, the number of defendants sentenced, and the length of those sentences.[10] Section 404(b) of the PRO IP Act also requests statistics on the number of arrests made. Please see the Annual Report of the Federal Bureau of Investigation, provided pursuant to Section 404(c) of the PRO IP Act, for an accounting of arrest statistics.

District Totals	FY 2016
Investigative Matters Received by AUSAs	243
Defendants Charged	104
Cases Charged	77
Defendants Sentenced	73

[9] https://www.bja.gov/ProgramDetails.aspx?Program_ID=64

[10] Case statistics were compiled by the EOUSA. The chart includes data on criminal cases/defendants where the following charges were brought as any charge against a defendant: 17 U.S.C. §506 (criminal copyright infringement); 17 U.S.C. §§ 1201 to 1205 (circumvention of copyright protection systems); 18 U.S.C. §§ 1831 (economic espionage) & 1832 (theft of trade 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 & 605 (signal piracy). The statutes were grouped together to eliminate double-counting of cases and/or defendants where more than one statute was charged against the same defendant. However, this chart may not include cases or defendants if only a conspiracy to violate one of these offenses was charged.

No Prison Term	41
1-12 Months	12
13-24 Months	8
25-36 Months	3
37-60 Months	6
60 + Months	3

In addition, we have provided the chart below with FY 2016 statistics for criminal IP cases broken down by type of charge.[11]

Charge	Cases charged	Percentage
Trademark *Trafficking in counterfeit goods, 18 U.S.C. § 2320*	55	71%
Copyright *Criminal copyright infringement, 17 U.S.C. §506* *Counterfeit labels, 18 U.S.C. § 2318* *DMCA, 17 U.S.C. § 1201*	 10 6 1	 13% 8% 1%
Economic Espionage Act *Economic espionage, 18 U.S.C. § 1831* *Theft of trade secrets, 18 U.S.C. § 1832*	 1 5	 1% 6%
Total	**78**	**100%**

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

The Criminal Division currently devotes seventeen full-time attorneys, along with paralegals and support staff, in CCIPS to IP issues. CCIPS also provides substantial support to the IPR Center, assigning at least one attorney, and sometimes more, to help identify and de-conflict investigative leads, as well as develop and execute national enforcement initiatives.

[11] 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.

The CHIP Network consists of AUSAs who are specially trained in the investigation and prosecution of IP and computer crimes. Every U.S. Attorney's Office has at least one CHIP attorney, and those districts that have historically faced the highest concentration of IP and high-tech crimes tend to have multiple CHIP attorneys.

Over the last year, approximately more than twenty NSD attorneys have worked on hacking investigations (most of which involve the theft of information, including but not limited to trade secrets). As described above, the NSCS Network consists of more than 100 AUSAs and attorneys at Department headquarters who receive specialized annual training in the investigation and prosecution of national security cyber offenses, including the theft of IP and other information.

Under the IPLEC program, DOJ has had a Department attorney stationed in Bangkok, Thailand, since January 2006 to handle IP issues in Asia. Between November 2007 and March 2011, a separate DOJ attorney was stationed in Sofia, Bulgaria, in order to handle IP issues in Eastern Europe. While funding for this position expired in 2011, DOJ has worked with the Department of State to post a DOJ attorney in Bucharest, Romania in 2015 to continue to handle IP issues in that region. DOJ also expanded its IPLEC program in FY 2015 by placing a DOJ attorney in Brasilia, Brazil, for a six-month term. With the assistance of the State Department, DOJ has continued to expand the IPLEC program in FY 2016 by posting new regional IPLECs in Hong Kong and Sao Paolo, Brazil. The State Department and DOJ expect to field a new IPLEC position in Abuja, Nigeria, in FY 2017.

The Cybercrime Lab housed in CCIPS provides support in evaluating digital evidence in IP cases, with a current total of nine 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.

IP 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' IP is infringed, including Uniform Domain-Name Dispute-Resolution Policy 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 and assisting AUSAs throughout the country with their counterfeit pharmaceutical and device cases.

(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-HSI, 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 ("NCIJTF"), 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.

Appendix A – Glossary

A2C2	Automotive Anti-Counterfeiting Council
AUSA	Assistant U.S. Attorney
BJA	Bureau of Justice Assistance
CBP	Customs and Border Protection
CCIPS	Computer Crime and Intellectual Property Section
CES	Counterintelligence and Export Control Section
CHIP	Computer Hacking and Intellectual Property
CODA	Content Overseas Distribution Association
DMCA	*Digital Millennium Copyright Act*
DOJ	Department of Justice
EOUSA	Executive Office for United States Attorneys
FBI	Federal Bureau of Investigation
FBI's Annual Report	FBI Fiscal Year 2016 Report to Congress on Intellectual Property Enforcement
FY 2016	Fiscal Year 2016
IC	Integrated circuits
ICE-HSI	Immigration and Customs Enforcement's Homeland Security Investigations
IP	Intellectual property
IPCEWG	IP Criminal Enforcement Working Group
IPEC	Intellectual Property Enforcement Coordinator
IPEP	Intellectual Property Enforcement Program
IPLEC	Intellectual Property Law Enforcement Coordinator
IPR Center	National IP Rights Coordination Center
JLG	U.S.-China Joint Liaison Group
NAC	National Advocacy Center
NCIJTF	National Cyber Investigative Joint Task Force
NSCS	National Security Cyber Specialists
NSD	National Security Division
NW3C	National White Collar Crime Center
OJP	Office of Justice Programs

OPDAT	Office of Overseas Prosecutorial Development, Assistance and Training
PGR	Procuraduría General de la República
PRC	People's Republic of China
PRO IP Act	*Prioritizing Resources and Organization for Intellectual Property Act of 2008*
USITC	U.S. International Trade Commission
USPTO	U.S. Patent and Trademark Office