United States Department of Justice

PRO IP Act
Annual Report FY 2017

PRO IP ACT ANNUAL REPORT OF THE ATTORNEY GENERAL FY 2017

INTRODUCTION

The Department of Justice (the "Department" or "DOJ")[1] submits this Fiscal Year 2017 ("FY 2017") 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 2017 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 2017 (*i.e.*, October 1, 2016 through September 30, 2017) are set forth below.

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 continues to participate 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 2017, 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, 2017, Pub. L. No. 115-31, 131 Stat. 135, 204, 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 2017, OJP was able to grant seven six awards totaling $2,048,304 to local and state law enforcement and prosecutorial agencies. The following FY 2017 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
2017-H0104-TX-BE	City of Austin	$400,000.00
2017-H0006-MD-BE	Baltimore, County of	$58,142.00
2017-H0105-CA-BE	City of Los Angeles	$400,000.00
2017-H0090-NC-BE	North Carolina Department of the Secretary of State	$400,000.00
2017-H0089-AZ-BE	City of Phoenix Police Department	$390,162.00
2017-H0095-MO-BE	City of Saint Louis Metropolitan Police Department	$400,000.00

Since the inception of the program, OJP has awarded $26,357,513 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 $19,058,849. Throughout the duration of the program, these agencies have made seizures totaling $532,228,560, which includes counterfeit merchandise and other property valued at $487,150,327, and $15,078,229 in currency.

In addition to these seizures, grantees engaged in the following law enforcement activities in the one-year period from July 1, 2016 to June 30, 2017:

• 423 individuals were arrested for violations of IP laws;
• 203 state and local IP search warrants were served; and
• 376 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 2016, the San Antonio Police Department ("SAPD") has seized over 33,285 items with a MSRP of over 1.2 million dollars in 2016. Between July 2016 and December 2016, the Department seized over 27,810 counterfeit items with a MSRP of over a million dollars and generated 112 prosecutable cases.

- In FY 2017, the Los Angeles Police Department's Anti-Piracy Unit served 15 search warrants and arrested 20 individuals for intellectual property related crimes and recovered over $9 million dollars in evidence value. The Anti-Piracy Unit provided intellectual property investigative technique training to 224 Law Enforcement Officers and conducted first-hand "ride-along" training to officers and prosecutors. The Anti-Piracy Unit provided training for Portland, Oregon, and Meza, Arizona, Police Departments on intellectual property investigative techniques.

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, 2016 and June 30, 2017, NW3C conducted these training sessions for 213 attendees from 86 agencies in 7 locations.[2] During this time, NW3C also conducted 6 technical assistance visits involving 61 agencies with 146 participants in order to improve their IP investigative and prosecutorial approaches.

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

- 97 trainings for 2,251 attendees from 1,164 agencies;
- 17 seminars for 573 attendees from 194 agencies; and
- 31 technical assistance visits for 396 attendees from 116 agencies.

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

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

Please see the FBI's Annual Report, which will be submitted separately pursuant to Section 404(c) of the PRO IP Act.

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

(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 2016, Congress did not appropriate funds to support Section 402(b) of the PRO IP Act in FY 2017.[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 2017, the Department has taken the following additional actions to address this important issue:

[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."

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 2017, 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 training and outreach activities are described in section (a)(7)(B) of this Report.

Executive Order

On February 9, 2017, President Trump issued an Executive Order on Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking. DOJ is working together in partnership with the Department of State, Department of Homeland Security, and the Office of the Director of National Intelligence to implement Executive Order 13773. As part of this implementation, DOJ will continue to address the links between transnational criminal organizations and IP crime.

(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 2017 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

The Department did not receive any authorizations under Sections 402 and 403 of the PRO IP Act in FY 2017.

(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. 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]

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 implementing the IPEC's FY2017-2019 Joint Strategic Plan ("JSP") on Intellectual Property Enforcement. As part of the JSP implementation, the Department participates in a variety of interagency working groups designed to address topics including engagement with private stakeholders; money laundering / criminal financing;

[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 2016 PRO IP Reports are available at the same location.

engagement with other countries; domestic application of the "Whole of Government" and "Specialized Office" approaches to IPR protection and enforcement; storage, destruction, and disposal of seized counterfeit goods; trade secrets / cybersecurity; and advancing the JSP's "Calls for Research."

CCIPS and CHIP Program

The Department carries out its overall IP criminal prosecution mission through the United States Attorneys' Offices and CCIPS, which works closely with a network of over 270 specially-trained federal prosecutors who make up the Department's Computer Hacking and Intellectual Property ("CHIP") program.

CCIPS is a section within the Criminal Division consisting of a specialized team of forty prosecutors who are devoted to enforcing laws related to computer and IP crimes. Fifteen 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. The IPLEC program has continued to expand, and with the assistance of the State Department, the DOJ has posted regional IPLECs in Bucharest, Romania; Hong Kong; Sao Paolo, Brazil; and 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

[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;

areas of responsibility including: (1) prosecuting computer crime and IP offenses; (2) serving as the district's legal counsel on matters relating to those offenses and the collection of electronic evidence; (3) training prosecutors and law enforcement personnel in the region; and (4) conducting public and industry outreach and awareness activities.

CES and the NSCS Network

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. In January 2017, CES released its "Strategic Plan for Countering the National Security Cyber Threat," which recognizes that our nation's adversaries are also stealing intellectual property through cyber-enabled means and proposes a strategy specifically designed to disrupt such efforts. NSD is currently in the process of implementing both plans.

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 legal and other 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.

Philadelphia, Pennsylvania; Pittsburgh, Pennsylvania; Sacramento, California; San Diego, California; San Jose, California; Seattle, Washington; and Washington, D.C.

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

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 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.

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

The Department achieved notable success in FY 201& both domestically and abroad. Some of these efforts are highlighted below:

Prosecution Initiatives

The Department continues to prioritize IP investigations and prosecutions 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 2017, this initiative resulted in a number of significant prosecutions, including those set forth below:

[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.

- *Two Sentenced for Trafficking in Counterfeit Viagra and Cialis.* On December 6, 2016, Martez Alando Gurley and Victor Lamar Coates were sentenced for trafficking in counterfeit Viagra and Cialis. Gurley was sentenced to 75 months in prison, and ordered to pay $410,508 in restitution to Pfizer Inc. and Eli Lilly and Company. Coates was sentenced to 46 months, and ordered to pay $314,565 in restitution. Gurley and Coates illegally imported the counterfeit tablets into the United States from sources in China.

- *Citizen of China Who Attempted Illegal Export of Advanced Military Computer Chips is Sentenced.* On December 20, 2016, Jiang Yan was sentenced to approximately 12 months of imprisonment for attempting to purchase and export to China, without a required license, certain sophisticated integrated circuits used in military satellites and missiles, and for conspiring to sell counterfeits of those same integrated circuits to a purchaser in the United States. According to court documents and statements made in court, Yan and co-conspirators Xianfeng Zuo, and Daofu Zhang each operated businesses in China that bought and sold electronic components, including integrated circuits ("ICs"). In November 2015, Zhang shipped from China, to a U.S. individual, two packages containing a total of eight counterfeit ICs, each bearing a counterfeit Xilinx brand label. Yan, Zhang, and Zuo flew together from China to the U.S. in early December 2015 to complete the Xilinx ICs purchase. Federal agents arrested all three at the meeting location. On March 7, 2016, Yan pleaded guilty to one count each of conspiracy to traffic in counterfeit goods, and attempted unlicensed export of export-controlled items. As part of his sentence, Yan was ordered to forfeit $63,000 in cash seized incident to his arrest. Yan will be deported to China. Zhang and Zuo also pleaded guilty and were each sentenced to 15 months of imprisonment on July 8, 2016, and November 4, 2016, respectively.

- *Owner Of Major Online Colored Contact Lens Business Sentenced to 46 Months in Prison for Importing and Selling Counterfeit and Misbranded Contact Lenses.* On January 18, 2017, Dmitriy V. Melnik was sentenced to 46 months in prison for running an international operation importing counterfeit and misbranded contact lenses from suppliers in Asia and then selling them over the internet without a prescription to tens of thousands of customers around the country. Melnik was ordered to remit $200,000 in restitution and forfeit $1.2 million in proceeds derived from the scheme as well as property seized during the investigation.

- *Defendant Sentenced for Trafficking in Counterfeit Labels for Veterinary Products.* On February 6, 2017, Allen Smith was sentenced to 37 months in prison for trafficking, and aiding and abetting in the trafficking, of counterfeit labels for Frontline Plus, Advantage, and K9 Advantix Plus products into and throughout the United States. Smith was also ordered to pay $867,150 in restitution and to forfeit $42,269 worth of illicit proceeds. Subsequently, on February 16, 2017, Lan Ngoc Tran was sentenced to 46 months in prison for trafficking in counterfeit labels for Frontline Plus veterinary products into and throughout the United States. Tran was also ordered to pay $867,150.44 in restitution and $841,813.94 in forfeiture. Previously, on July 9, 2015, a grand jury indicted four leading members of an organized crime group, including Smith and Tran, for trafficking and smuggling in millions of counterfeit veterinary products into and throughout the United States. The group represents the largest known suppliers of counterfeit packaging for flea treatment products in the United States. On December 20, 2013, HSI agents executed a search warrant and raided the business

location of Chris Martin, co-defendant with Smith, who was the sole supplier of Frontline Plus flea treatment products to Target department stores, as well as a supplier to other major retail outlets for flea treatment products. Target removed from the shelves of all its nationwide stores all products purchased from Martin, including the Frontline Plus, Advantage, and K9 Advantix Plus products. On January 5, 2018, Martin was sentenced to 47 months in prison, and ordered to pay $867,150.44 in restitution and forfeit $42,269.10.

- *Joint Law Enforcement Operation Leads to Conviction of Counterfeit Drug Manufacturers.* On February 7, 2017, David Beckford was sentenced to more than 10 years in prison for his role in a conspiracy to manufacture counterfeit Xanax pills, for engaging in international money laundering, and for his use and possession of a firearm in furtherance of drug trafficking and in violation of the felon-in-possession statute. According to the guilty plea, Beckford admitted that from January 17, 2014, through December 12, 2015, he engaged in a scheme to import controlled substances from China and other foreign sources, obtain manufacturing equipment, including a press to make pills, and press fake Xanax pills at locations in the Northern District of California. Subsequently, on July 28, 2017, Antoine King was sentenced to 30 months in prison and 3 years of supervised release for his role in the conspiracy to manufacture counterfeit Xanax pills and to launder the proceeds gained by the illegal scheme. According to the guilty plea, King admitted that from October 6, 2014 through December 12, 2015, he was involved in a conspiracy with co-conspirator David Beckford and others to manufacture and distribute pills that were designed to resemble Xanax pills as nearly as possible.

- *Defendant Sentenced for Trafficking in Counterfeit Pharmaceuticals*. On March 10, 2017, Robert Grabau was sentenced to three years of probation for trafficking in counterfeit Viagra, and attempting to distribute and possess with intent to distribute phentermine, a Schedule IV controlled substance. Grabau must also forfeit over 41,000 pills of alprazolam and counterfeit Viagra, pay a money judgment of $38,500, and pay $100,000 in restitution to Pfizer Corporation.

- *Plea of Guilty for Selling Counterfeit Airbags Online.* On May 31, 2017, Vitaliy Fedorchuk pleaded guilty to five counts of mail fraud for an international scheme to sell counterfeit airbags via ebay and other online sites. According to court documents, between June 23, 2014, and July 27, 2016, Fedorchuk offered for sale airbag modules, covers, and manufacturer emblems at his ebay online store, redbarnautoparts. Fedorchuk falsely advertised that the counterfeit airbags were original equipment from major automobile manufacturers such as Honda, Fiat, Chrysler, Nissan, Toyota, GMC and Ford. During the scheme, Fedorchuk sold hundreds of counterfeit airbags and obtained more than $95,000. According to the plea agreement, all airbag parts Fedorchuk sold through his online store were counterfeit. On October 5, 2017, Fedorchuk was sentenced to one year and one day in prison.

- *Counterfeiters Sentenced For Convictions In Nationwide Conspiracy To Distribute Fake 5-Hour Energy Drink.* On June 20, 2017, Joseph Shayota and his wife, Adriana Shayota, were sentenced for their roles in a conspiracy to traffic in counterfeit goods and conspiracy to commit criminal copyright infringement and to introduce misbranded food into interstate commerce. Joseph Shayota was sentenced to 86 months, and Adriana Shayota to 26 months

imprisonment. Their sentences brought an end to all but one of the cases brought against 11 defendants charged in a scheme involving the manufacture and sale of millions of bottles of the liquid dietary supplement 5-Hour ENERGY.

- *Distributor of Counterfeit Medications Arrested.* On September 22, 2017, Carolina Aguilar Rodriguez aka "Doctora," pleaded guilty to conspiracy to smuggle prescription drugs into the United States and receiving and delivering misbranded drugs with the intent to defraud. The criminal complaint alleged that she sold counterfeit Diprospan to undercover federal agents on at least five occasions. According to the charges, Rodriguez was not licensed to dispense prescription medications in Texas, and Naturavida was not licensed as a Texas pharmacy. Diprospan is not approved for use or sale in the United States and is not manufactured in the United States. Sentencing is scheduled for April 20, 2018.

- *Indictment on Federal Charges for Counterfeit Oxycodone Pills Containing Fentanyl and Synthetic Opioids.* On July 11, 2017, Cathine Lavina Sellers was charged with possession with the intent to distribute a controlled substance, involving fentanyl, a Schedule II controlled substance, and furanyl-fentanyl and U-47700, both of which were designated by DEA as a Schedule I controlled substance on an emergency basis in 2016. On June 13, 2017, Sellers allegedly sold approximately 100 pills for $1,400 in cash from her townhouse to a confidential source working with the DEA. A field test of the pills was positive for the presence of furanyl-fentanyl, which is an analog of fentanyl, similar to morphine but more potent. In conjunction with this arrest, the U.S. Attorney's Office and Atlanta DEA have issued a public warning regarding these counterfeit pills through their public affairs offices as well as through the North Georgia Heroin Working Group.

- *Two Indian Nationals Charged with Smuggling Counterfeit Cigarettes into the United States.* On August 24, 2017, Abhishek Shukla and Harish Shabhai Panchal, along with two companies incorporated in India, Jubilee Tobacco Industries Corp., and Pelican Tobacco (India) Private Limited, were charged with conspiring to smuggle counterfeit cigarettes into the United States. The defendants were charged with trafficking in counterfeit goods and with selling counterfeit tobacco products with false labeling. The indictment alleges that approximately 68,600 cartons of counterfeit Newport brand cigarettes were shipped into the United States, which were seized in two shipments at the Port of Miami. The defendants are pending trial in the Southern District of Florida. If distributed in the State of Florida, the un-taxed shipments would have an approximate value of approximately $4.3 million.

- *Guilty Pleas for Conspiracy to Traffic Counterfeit Steroids.* On August 28, 2017, Tyler Bauman pleaded guilty to conspiracy to distribute counterfeit testosterone, trenbolone, and other steroid compounds; conspiracy to traffic in counterfeit drugs; conspiracy to launder money; possession with intent to distribute controlled substances (steroids); and trafficking in counterfeit drugs. In April 2017, Bauman and five others were arrested and charged with various offenses related to the steroid operation. According to court documents, from approximately May 2015 until April 12, 2017, the defendants manufactured steroid products - made from raw materials purchased overseas - and marketed them as "Onyx" steroids using "Onyx" labels that were also ordered from overseas suppliers. Bauman is scheduled to be sentenced in January 2018. Previously, on June 21, 2017, co-conspirator Robert Medeiros pleaded guilty to one count of conspiracy to traffic in counterfeit drugs and to distribute

controlled substances. Medeiros' principal role in the conspiracy was to fulfill orders for anabolic steroids by obtaining the finished steroid products, branded with Onyx labeling and packaging, from other members of the conspiracy, prepare the steroids for shipment, and ship the steroids via the U.S. Postal Service to customers across the United States. Additionally, on July 14, 2017, co-conspirator Melissa Sclafani pleaded guilty to one count of conspiracy with intent to distribute and distribute counterfeit steroids and one count of conspiracy to launder money. Sclafani obtained materials and supplies to manufacture the counterfeit steroids and served as the corporate secretary of Wicked Tan LLC, a tanning business owned by two co-conspirators. Sclafani assisted members of the conspiracy in laundering proceeds from the sale of counterfeit steroids through the business.

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

In FY 2017, 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 thefts and economic espionage cases. Recent cases include:

- *Two Men Charged with Stealing Trade Secrets from Defense Contractor.* On November 3, 2016, Jared Dylan Sparks and Jay Williams were charged by indictment with offenses related to a scheme to steal trade secrets from a Connecticut-based defense contractor. According to court documents and statements made in court, Sparks, an electrical engineer, and Williams, an electronic technician, both worked at LBI Inc., a Connecticut-based defense contractor that designs and builds, among other things, unmanned underwater vehicles for the U.S. Navy Office of Naval Research. Information obtained from the execution of various search warrants revealed that beginning in at least May 2011 and continuing until November 2011, Williams and Sparks, without authorization, uploaded LBI proprietary information to Dropbox online file storage accounts. Trial is scheduled to begin on March 13, 2018.

- *Agricultural Scientist Convicted in Theft of Engineered Rice.* On February 16, 2017, Weiqiang Zhang was convicted on one count of conspiracy to steal trade secrets, one count of conspiracy to commit interstate transportation of stolen property and one count of interstate transportation of stolen property. Evidence at trial established that Zhang worked as a rice breeder for Ventria Bioscience. Ventria develops genetically programmed rice to express recombinant human proteins, which are then extracted for use in the therapeutic and medical fields. According to trial evidence, Zhang acquired without authorization hundreds of rice seeds produced by Ventria and stored them at his residence in Manhattan. On August 7, 2013, U.S. Customs and Border Protection officers found seeds belonging to Ventria in the luggage of Zhang's visitors as they prepared to leave the United States for China.

- *Russian Federal Security Service (FSB) Officers and Criminal Hacker Charged With Economic Espionage Targeting Yahoo, Inc.* On February 28, 2017, three Russian nationals, including two FSB officers, were charged with economic espionage in relation to a widely publicized breach at Yahoo that resulted in the theft of Yahoo trade secrets and account information for more than 500 million Yahoo accounts and with unauthorized access to the contents of more than 30 million accounts, primarily at Yahoo. FSB officer Dmitry

Dokuchaev (who was from the FSB unit that is the FBI's point of contact in Moscow for cybercrime) and his FSB superior, Igor Sushchin, used one of FBI's "Most Wanted" criminal hackers, Alexsey Belan, to gain access to Yahoo's network and trade secrets. All three men then used this access to hack email accounts of Yahoo users, from Russian dissidents to foreign businesspeople.

- *New Jersey Man Charged With Theft Of Trade Secret Materials From Dupont.* On April 7, 2017, Anchi Hou was arrested and charged by complaint with one count of theft of trade secrets. According to the documents filed in this case and statements made in court, in the summer and fall of 2016, Hou allegedly copied and removed thousands of files containing DuPont's proprietary information, including formulas, data, and customer information related to flexographic printing plate technology. A forensic review of Hou's personal computer revealed that it contained more than 20,000 stolen DuPont files related to the company's flexographic printing plate technology. Some of the stolen files include information that DuPont considers trade secrets developed by its employees over the course of the past 40 years and which are critical to its technical, economic, and business operations.

- *Seven People Charged With Conspiring to Steal Trade Secrets For Benefit of Chinese Manufacturing Company.* On May 23, 2017, two defendants were arrested in Washington, D.C., three in the Southern District of Texas, and one in the District of Massachusetts. All six defendants were charged by criminal complaint in the U.S. District Court for the District of Columbia with conspiracy to commit theft of trade secrets, and a seventh defendant – a Chinese national living in China – also was charged. Between in or about 2012 and the present, the affidavit alleges that the Chinese manufacturer and employees of its Houston-based company engaged in a systematic campaign to steal the trade secrets of a global engineering firm that was a leader in marine construction technology. Subsequently, on June 8, 2017, all seven defendants were charged with conspiracy to steal trade secrets in an indictment. On December 15, 2017, Johnny Randall pleaded guilty to this conspiracy charge, and is scheduled to be sentenced on March 16, 2018.

- *Individual Charged with Economic Espionage for Stealing Source Code from Former Employer with Intent to Benefit the Chinese Government*. On May 19, 2017, Jiaqiang Xu pleaded guilty to theft of trade secrets and economic espionage. The six-count indictment returned in June 2016 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. Xu is scheduled to be sentenced on January 18, 2018.

- *Chinese National Sentenced for Economic Espionage for Stealing Sensitive Military Program Documents from U.S. Defense Contractor*. On June 22, 2017, Yu Long was sentenced to approximately 30 months for his theft of voluminous sensitive military program documents from U.S. defense contractor United Technologies (UTC) and transporting them

to China. After attending U.S. universities, Long worked for six years as a senior engineer at UTC on F119 and F135 airplane engines. Beginning in 2013, Long was recruited, through PRC Talent Programs, to return to China to work on research projects at certain state-run universities, using knowledge and materials he had acquired while employed at UTC. Long brought with him and accessed in China a UTC external hard drive that had been issued to him and that he unlawfully retained. A review of Long's digital media seized at the time of his arrest revealed voluminous files controlled under the International Traffic in Arms Regulations and Export Administration Regulations, and voluminous files proprietary to various U.S. companies.

- *Former Lutonix Executive Sentenced For Stealing Trade Secrets.* On August 17, 2017, Christopher Barry was sentenced to 12 months and 1 day in prison for stealing trade secrets from his former employer, Lutonix. Barry was also ordered to pay $533,842 in restitution to Lutonix. Barry pleaded guilty to a felony information on April 5, 2017. According to the defendant's guilty plea, in May 2015, Barry left Lutonix and accepted employment as CEO of Urotronic, a start-up medical device company founded by a former Lutonix employee. As Barry was planning to leave Lutonix, he stole numerous trade secret files belonging to the company so that he could utilize the proprietary information in connection with his next job.

- *Former Chemours Employee Charged With Conspiracy To Steal Trade Secrets In Connection With Plan To Sell Trade Secrets To Chinese Investors.* On September 5, 2017, Jerry Jindong Xu, a former Chemours employee, was charged by a federal grand jury with conspiring to steal trade secrets and attempting to monetize them with Chinese investors. According to the indictment, the conspiracy involved sodium cyanide, a chemical used in mining and for which Chemours is the world's largest producer. Xu, who moved from China to North America in 2011 while employed by DuPont, became a Chemours employee when Chemours spun off of DuPont in 2015.

(3) Large-Scale Commercial Counterfeiting and Online Piracy

The Department continues to pursue significant, large-scale piracy and counterfeiting operations. In FY 2017, the Department has had a number of significant prosecutions, including those set forth below:

- *Fourth Conspirator in SnappzMarket Android Mobile Device App Piracy Group Convicted of Conspiracy to Commit Criminal Copyright Infringement.* On June 19, 2017, Joshua Taylor was sentenced to 16 months in prison for conspiracy to commit criminal copyright infringement. Taylor was the fourth member of the SnappzMarket online piracy group convicted for his role in the illegal distribution of copies of copyrighted Android mobile device applications ("apps"). Evidence presented at trial demonstrated that Taylor and his co-conspirators identified themselves as members of the SnappzMarket Group, which reproduced and distributed copies of copyrighted Android mobile device apps between May 2011 and August 2012. Previously, on February 10, 2017, Kody Peterson, a leading member of the SnappzMarket group, was sentenced to a year and a day in prison for conspiring to commit criminal copyright infringement by reproducing and distributing paid Android apps on a massive scale to group members across the globe. Peterson was also ordered to pay a statutory fine of $15,000. Scott Walton, another co-conspirator, was sentenced to 46 months

in prison in August 2016. Additionally, Gary Edwin Sharp II pleaded guilty on January 13, 2016 and is scheduled for sentencing in March 2018. The FBI also executed a seizure order against the group's website. The total retail value of the more than one million pirated apps distributed by the SnappzMarket Group was estimated at more than $1.7 million.

- *Defendants Plead to Trafficking in Counterfeit Goods, Labels, and Packaging.* On February 22, 2017, defendants Andreina Becerra, Roberto Volpe, and Rosario LaMarca pleaded guilty to conspiracy to traffic in counterfeit goods, labels, and packaging; conspiracy to smuggle goods into the United States; and conspiracy to structure financial transactions as well as substantive counts of those offenses. From July 2009 to October 2013, the defendants allegedly trafficked more than 40,000 electronic devices bearing counterfeit Apple and Sony trademarks, including iPods, iPhones, and iPads, as well as their accompanying accessories, labels, and packaging from Hong Kong and the People's Republic of China to multiple locations throughout the United States. The estimated manufacturer's suggested retail price for these items exceeds 15 million dollars. LaMarca was sentenced to 37 months in prison on July 20, 2017.

- *Guilty Plea in Software Piracy Scheme.* On March 2, 2017, David Reece pleaded guilty to a federal information that charged him with conspiracy. Reece admitted that he conspired with others – including Casey Lee Ross and another individual in the People's Republic of China – to smuggle illegal merchandise into the United States and distribute it to others. Reece bought and sold illicit and/or unauthorized Microsoft Office product key cards. (Product key cards contain codes that are used to obtain full access to licensed versions of copyrighted Microsoft software programs, in this case, purportedly for Lenovo computers.) At an estimated loss of $250 per item, this constitutes a total loss of approximately $2.5 million. Reece is the eighth defendant charged in the software piracy scheme and the seventh defendant to plead guilty.

- *Member of CD and DVD Counterfeiting Ring Sentenced to 60 Months in Prison.* On March 22, 2017, Mamadou Aliou Simakha was sentenced to 60 months in prison and ordered to pay $70,894 in restitution, jointly and severally with his co-defendants. Simakha pleaded guilty on March 10, 2010, to one count of conspiracy to commit criminal copyright infringement, to traffic in counterfeit goods and to traffic in counterfeit labels. After entering his guilty plea, Simakha fled the country, and a warrant was issued for his arrest on April 6, 2010. On March 1, 2016, Simakha was arrested in Morocco and was extradited from Morocco into the custody of the U.S. Marshals Service on Dec. 15, 2016. Simakha was one of 13 individuals charged by a federal grand jury on May 19, 2009, in an indictment alleging various copyright, trademark and counterfeit label offenses.

- *Sentence for Trafficking in Counterfeit Goods.* On May 3, 2017, Kurt Michael Krol was sentenced to 72 months imprisonment. Additionally, Krol agreed to forfeit to the government all counterfeit articles seized; over $200,000 in proceeds seized from six locations; and a money judgment in the amount of the gross proceeds of the offense. The investigation revealed that on January 22, 2008, Krol founded Universal Mania, Inc. (UM), an internet based marketplace. Krol met with a representative from a Chinese company that counterfeited Otterbox products in Fayetteville to find out what other products they could counterfeit. Krol sold counterfeit merchandise, as well as merchandise from legitimate

distributors on the internet. He comingled the sales proceeds from the counterfeit products with proceeds from legitimate sales.

- *Two Individuals Sentenced Federally for Importing Counterfeit Microsoft Software Into The United States.* On May 23, 2017, Clifford Eric Lundgren was sentenced to 15 months in prison and a $50,000 fine, and Robert J. Wolff was sentenced to 6 months house arrest and four years of probation. Lundgren and Wolff previously pled guilty to participating in a conspiracy to traffic in counterfeit goods, and committing criminal copyright infringement. According to documents filed with the court, Lundgren and Wolf manufactured and imported 28,000 discs containing Microsoft Windows programming, specifically, 7 Dell reinstallation Edition and XP Service Pack 3 Dell reinstallation Edition. Lundgren and Wolff violated Microsoft's intellectual property rights by illegally manufacturing the software in China and then importing the discs into the United States.

- *Chinese National Indicted for Trafficking Counterfeit Computer Networking Equipment.* On July 19, 2017, a grand jury returned an indictment charging Ruiyang Li with trafficking in and smuggling counterfeit HP, Cisco, and Intel computer networking equipment. Li was arrested on July 7, 2017, upon entering the United States at Los Angeles International Airport (LAX). According to the allegations in the indictment, Li has been trafficking in counterfeit goods since 2007, causing millions of dollars in losses to the victim companies. Li pleaded guilty on December 8, 2018, and sentencing is scheduled for March 30, 2018.

- *Guilty Pleas for Copyright Infringement of Microsoft Products And Conspiracy To Commit Wire Fraud.* Robert F. Stout and Kasey N. Riley pleaded guilty on August 8, 2017, to copyright infringement and conspiracy to commit wire fraud relating to the sale of illegal activation keys for Microsoft products. The United States is seeking a money judgment in the amount of $1,480,227, the proceeds of the charged criminal conduct. Stout was sentenced to 18 months in prison, and Riley was sentenced to probation on December 1, 2017.

- *Chinese National Pleads Guilty to Software Piracy Scheme.* On September 19, 2017, Wen Tao Liu pleaded guilty to one count of conspiracy and one count of trafficking in counterfeit labels. Investigators have seized more than $20 million in assets from defendants in several separate but related cases, who are estimated to have sold in excess of $100 million worth of illicit, unauthorized and counterfeit software products to thousands of online customers. Liu, doing business as Haitu International Group Co. Limited (an entity based in Hong Kong), participated in a conspiracy with Casey Lee Ross of Kansas City, Mo. (doing business as Software Slashers), David Reece of Fort Lauderdale, Fla., and others from March 10, 2010, to February 2, 2015, to commit the offenses of unauthorized solicitation of access devices, trafficking in counterfeit goods and smuggling goods into the United States.

- *Staten Island Man Admits Trafficking Over $2.5 Million In Counterfeit Footwear Through Port Of Newark.* On September 26, 2017, Shi Wei Zheng pleaded guilty, admitting his plan to distribute more than $2.5 million of counterfeit UGG-brand boots shipped into the Port of Newark. From September 2016 through February 2017, Zheng received certain shipping container numbers from an individual overseas that identified at least three containers containing counterfeit UGG boots. Cheng asked individuals working at the Port of Newark to remove the containers from the port before they could be examined by U.S. Customs and Border Protection. Once the containers were removed, Zheng directed that they be delivered

to other individuals working for him, who would then distribute the boots in New Jersey and elsewhere. Before Zheng could distribute the goods, law enforcement intercepted the containers, examined their contents, and determined the boots were counterfeit.

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 2016, 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 January 2017, CCIPS and NSD organized and taught DOJ's Economic Espionage and Trade Secrets Seminar at the National Advocacy Center in Columbia, South Carolina, Approximately 80 prosecutors and law enforcement agents from around the country attended the course, which featured in-depth presentations on investigating and prosecuting theft of trade secrets and economic espionage cases.

- In March, June, and August 2017, CCIPS presented at an Intellectual Property and Trade Enforcement Investigations course at the National Intellectual Property Rights Coordination Center in Crystal City, Virginia, to approximately 30 HSI and CBP agents. The presentation covered relevant law and policy, practical guidance in counterfeit trademark investigations, and included a case study of *U.S. v. Peter Picone*, a defendant convicted of selling counterfeit integrated circuits to the U.S. Navy for use in a nuclear submarine.

- In March 2017, CCIPS presented on "Collaborating with the Department to Fight IP Crime and Cybercrime" at the Corporate Counsel Forum in Indianapolis, Indiana. Hosted by FBI Indianapolis and the U.S. Attorney's Office for the Northern and Southern Districts of Indiana, the Corporate Counsel Forum is intended to educate corporate counsel on the mission of the DOJ and FBI. Approximately 75 organizations attended the event.

- In March 2017, 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 May and September 2017, 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 August 2017, CCIPS participated in the International Law Enforcement IP Crime Conference at the United Nations Headquarters located in New York. The event brought together approximately 600 police, customs, prosecutors, and other government officials as well as rights holders representing a wide variety of industries to share best practices, create stronger networks to combat IP crime, and develop joint initiatives focused on enforcement, education and partnerships. Deputy Attorney General Rod Rosenstein provided a keynote address at the conference.

- In September 2017, CCIPS presented at the Naval Criminal Investigative Service's (NCIS's) 2017 Economic Crimes Conference at Quantico, Virginia. CCIPS discussed methods for the investigation and prosecution of cases involving counterfeit microelectronics and presented case studies. Approximately 75 NCIS agents and analysts attended the three-day training conference.

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 2017, 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 2017 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 2017, the Department, with the assistance from the State Department, continued to expand the IPLEC program. Experienced DOJ attorneys now serve as regional IPLECs in Bangkok, Thailand; Bucharest, Romania; Hong Kong; Sao Paolo, Brazil; and Abuja, Nigeria.[8]

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

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

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

ASIA

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 2016, CCIPS participated in the 14th 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 August 2017, 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. Representatives from the National IPR Center, ICE-HSI Beijing & New York, and FBI also attended the meeting on behalf of the United States.

U.S. Patent and Trademark Office's Intellectual Property Enforcement Roundtable for Chinese Officials. In October 2016, CCIPS participated in a roundtable discussion on the U.S. government's enforcement of intellectual property laws, as part of a one-day seminar hosted by the U.S. Patent and Trademark Office's ("USPTO's") Global Intellectual Property Academy in Alexandria, Virginia. The audience consisted of 25 Chinese officials from provincial and central enforcement agencies.

U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues. In December 2016, Attorney General Loretta E. Lynch and Department of Homeland Security Secretary Jeh Johnson, together with Chinese State Councilor Guo Shengkun, co-chaired the third U.S.-China Joint Dialogue on Cybercrime and Related Issues. The dialogue aimed 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 pragmatic bilateral cooperation with regard to cybercrime, network protection and other related issues. At the dialogue, both sides agreed to continue to cooperate on the investigation of cybercrime and malicious cyber activities emanating from China or the United States and to refrain from cyber-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors. As a result, both sides plan to continue evaluating the effectiveness of case cooperation, focus cooperation on hacking and cyber-enabled fraud cases, share cybercrime-related leads, expand cyber-enabled crime cooperation to counter Darkweb marketplaces, and provide concrete and timely updates on cases brought within the ambit of the dialogue, among other agreements.

5th Intellectual Property Crimes Enforcement Network (IPCEN) Meeting. In February 2017, CCIPS, the Bangkok IPLEC, and the Hong Kong IPLEC organized and participated in the 5th IPCEN meeting held in Bangkok, Thailand. The meeting facilitated the exchange of successful investigation and prosecution strategies in combating domestic and cross-border copyright piracy and trademark counterfeiting crimes. Over 50 prosecutors and law enforcement officers shared best practices and lessons learned in addressing retail and online counterfeiting and piracy, mass production and distribution of counterfeit goods, and border enforcement strategies. The IPCEN meeting also served to strengthen communications channels to promote coordinated, multinational prosecutions of the most serious offenders. Participating countries included Burma, Cambodia, Indonesia, Laos, Malaysia, Singapore, South Korea, Thailand, and Vietnam.

Presentation to Chinese Judges on Intellectual Property Rights. In March 2017, CCIPS addressed a visiting group of Chinese judges in Washington, D.C. on U.S. criminal enforcement of IP rights. The presentation was a part of the U.S. State Department's International Visitor Leadership Program.

Presentation to Chinese Delegations on U.S. Enforcement of Intellectual Property Rights. In March 2017, CCIPS addressed a visiting group of Chinese government officials, academics, and lawyers in Washington, D.C. on U.S. criminal enforcement of IP rights. The presentation was a part of the U.S. State Department's International Visitor Leadership Program.

Asia Regional Intellectual Property Rights (IPR) Criminal Enforcement Workshop. In March 2017, the Hong Kong IPLEC, with the assistance of CCIPS, organized the first Asia Regional IPR Criminal Enforcement Workshop in Hong Kong. Approximately 50 IP prosecutors and investigators from thirteen countries (United States, Bangladesh, Burma, China, India, Indonesia, Mongolia, Nepal, Pakistan, Sri Lanka, Thailand, Vietnam, and Hong Kong) gathered to discuss methods to facilitate the exchange of successful investigation and prosecution strategies in combating trademark counterfeiting, copyright infringement, and theft of trade secrets, and how to strengthen communication channels to promote coordinated, multinational prosecutions of the most serious offenders. The meeting included panel discussions and case studies by law

enforcement officials, presentations by representatives of affected industries, and technical and legal discussions from U.S. experts.

Intellectual Property Rights Law Enforcement Workshop for Pakistan. In July 2017, CCIPS presented to Pakistani law enforcement and intellectual property enforcement officials at the Intellectual Property Rights Law Enforcement Workshop for Pakistan. The hour-long presentation focused on intellectual property enforcement efforts, case studies and CCIPS' international assets and coordination efforts.

International Law Institute (ILI) 2017 China Law Society. In July 2017, CCIPS presented to the ILI's China Law Society. The delegation consisted of Chinese professors, legislators, and policy-makers. CCIPS's presentation focused on U.S. criminal intellectual property enforcement with a concentration on IP-related statutes, effective IP enforcement strategies, and coordination between prosecutors and investigative agencies. The presentation also provided case highlights, CCIPS resources, and trial strategies.

China IP Road Shows. In July 2017, DOJ CHIP AUSAs presented at China IP Road Shows, sponsored by the USPTO, in Detroit and Grand Rapids, Michigan. With the China IP Road Shows, the USPTO is partnering with a variety of organizations across the country — including universities, USPTO regional offices, business groups, state and local governments, and other federal agencies — to present a series of one-day events that delve into the details of how to better protect intellectual property (IP) in China. These one-day events bring to local businesses and stakeholders the expertise and knowledge of the USPTO's China specialists as well as that of special invited guests, and have been tailored to address the needs of the specific locale in which it is held.

Presentation to Chinese Delegation on IP Enforcement. In August 2017, CCIPS presented to a delegation of 26 Zhejiang Police College students from Zhejiang, China. CCIPS discussed DOJ's role in IP enforcement and on investigating and prosecuting IP crimes in the United States. The University of Maryland's Office of International and Executive Programs organized the delegation's visit.

ASEAN Network of IP Enforcement Experts (ANIEE) Meeting. In September 2017, the Hong Kong IPLEC participated in the ANIEE meeting hosted in Bangkok, Thailand. The meeting focused on initiatives related to enforcement under the 2016-2025 ASEAN IPR Action Plan. Initiatives included the development of information-sharing networks among government officials responsible for IP enforcement (customs, police, prosecutors, administrative enforcement authorities), and enhanced IPR border enforcement. Participating countries included Brunei, Burma, Cambodia, Malaysia, Indonesia, Laos, the Philippines, Singapore, Thailand, and Vietnam.

Regional Workshop on Effective Practices in Border Enforcement of Intellectual Property Rights. In September 2017, the Hong Kong IPLEC participated in the Regional Workshop on Effective Practices in Border Enforcement of Intellectual Property Rights in Bangkok, Thailand. The goal of the workshop was to support the participating countries' efforts to develop and enforce effective border strategies for targeting trademark and copyright infringing goods.

Participating countries included the United States, Bangladesh, Bhutan, Brunei, Burma, Cambodia, China, Timor-Leste, Hong Kong, India, Indonesia, Laos, Malaysia, Maldives, Mongolia, Nepal, Pakistan, Singapore, Sri Lanka, the Philippines, Thailand, and Vietnam.

U.S. Patent and Trademark Office's China IP Update. In September 2017, CCIPS spoke at the United States Patent and Trademark Office's (USPTO's) China IP Update Program in Alexandria, Virginia. The event provided an opportunity for U.S. government attendees to hear about the latest developments on a wide range of Chinese IP issues from U.S. government subject matter experts from agencies including the USPTO, USTR, Commerce, DOJ, FBI, HIS, and CBP. CCIPS spoke on a panel addressing recent updates on law enforcement cooperation with China.

NORTH AFRICA AND THE MIDDLE EAST

Intellectual Property Crime Workshop for Kazakhstan Delegation: In March 2017, CCIPS presented to a visiting delegation of 18 investigators and prosecutors from Kazakhstan as part of the Global Intellectual Property Academy's "Workshop on the Investigation and Prosecution of Intellectual Property Crimes," organized by the U.S. Patent and Trademark Office. CCIPS provided presentations addressing U.S. criminal investigation and prosecution procedure, computer forensic and electronic evidence issues, criminal prosecution of IP crimes, prosecution of trade secret theft cases, and sentencing and asset forfeiture issues as well as a case study.

Workshop for Azerbaijani Judges. In April 2017, CCIPS participated in a three-day training conference in Baku, Azerbaijan for approximately Azerbaijani judges focusing on protection of intellectual property rights. USPTO organized the conference in conjunction with the U.S. Embassy in Baku, DOJ, and the Azerbaijani judiciary. CCIPS gave five presentations on various topics involving intellectual property and IPR enforcement in the U.S. and Azerbaijan.

Regional IPR Enforcement Training in Jordan. In September 2017, CCIPS participated in training in Amman, Jordan, with law enforcement officials and attorneys from Egypt, Jordan, Lebanon, Morocco, Saudi Arabia, and United Arab Emirates. The regional workshop on investigating and prosecuting intellectual property violations brought together over 40 investigators and prosecutors to develop laws and procedures that will enhance regional ability to investigate and prosecute crimes involving intellectual property violations.

Regional IPR Enforcement Training in Senegal. In September 2017, the Nigeria IPLEC participated in training hosted in Dakar, Senegal. Customs officials, police officers, and prosecutors from Liberia, Sierra Leone, Gambia, Benin, Guinea and Senegal participated. The training emphasized the health and safety issues associated with counterfeit goods and their connection to transnational organized crime. The program focused on interdiction, investigations and enforcement operations, with emphasis on health and safety concerns of counterfeit goods such as pharmaceuticals, health and beauty products, and consumer electronics.

IPR Training Program for Moroccan Judicial Officials. In September 2017, CCIPS participated in two judicial exchange programs for approximately 60 Moroccan judges in Casablanca and Marrakesh, Morocco. The USPTO-sponsored programs highlighted the growing importance of

intellectual property in the Moroccan, U.S., and global economies, and for effective IP enforcement. CCIPS discussed various issues related to criminal IP enforcement, particularly online investigations.

CENTRAL AND SOUTH AMERICA

Meeting with Mexican Intellectual Property Attorneys. In October 2016, CCIPS Attorneys met in Washington, DC with nine attorneys from the Mexican Association for the Protection of Intellectual Property ("AMPPI") regarding IPR issues in Mexico and the U.S. The participants had a wide-ranging discussion focusing on how right holders could work more effectively with law enforcement in Mexico on IPR enforcement matters. Following the discussion, the delegation toured the CCIPS Cybercrime Lab and were provided an overview of the role and capabilities of the Lab. AMPPI had a follow-up meeting with DOJ the following week when a CCIPS attorney was in Mexico City as a presenter at a training conference for Mexican judges on intellectual property crimes and the accusatory system.

Training Conference in Mexico City for Mexican Judges. In October 2016, CCIPS and the Brazil IPLEC participated in a two-day training conference in Mexico City, Mexico for Mexican judges focusing on protecting IPR and Mexico's transition to an accusatory criminal justice system. DOJ, USPTO, and the U.S. Embassy in Mexico City organized the conference for over 70 participants including two U.S. federal judges. CCIPS gave a presentation regarding investigating, prosecuting, and adjudicating IPR cases in Mexico.

Intellectual Property Rights Enforcement Training in Brazil. In March 2017, the Brazil IPLEC participated in training with Brazilian law enforcement in Belo Horizonte, Brazil. The goal of the training was to strengthen the ability of Brazilian state and federal law enforcement officials in Minas Gerais (Belo Horizonte) to combat IP crime more effectively. The training consisted of U.S. and Brazilian case studies, overviews of USG resources and best practices in IP crime investigation and prosecution, and presentations from different rights-holders on their brand protection strategies and methods.

Intellectual Property Rights Enforcement Training in Peru. In April 2017, the Brazil IPLEC participated in training with Peruvian law enforcement in Lima, Peru. The goal of the training was to strengthen the ability of Peruvian law enforcement officials in Peru to combat digital IP crime more effectively. The training consisted of U.S. and Peruvian case studies, overviews of USG resources and best practices in IP crime investigation and prosecution, and presentations from different rights-holders on their brand protection strategies and methods.

Regional Intellectual Property Rights Enforcement Training in Panama. In August 2017, the Brazil IPLEC participated in training in Panama City, Panama, with law enforcement officials and attorneys from Panama, the Dominican Republic, Costa Rica, El Salvador, Guatemala, Honduras, and Mexico. This program focused on hard goods and the best practices for using effective tools to increase seizures, as well as how to investigate and prosecute these crimes successfully in a challenging legal environment. The participants were primarily law enforcement, prosecutors, and customs officers.

EUROPE

EUIPO-CEPOL Workshop. In October 2016, CCIPS participated in and spoke at the "EUIPO-CEPOL Counterfeiting Goods and Intellectual Property" Conference in Paris, France. The European Union Intellectual Property Office (EUIPO) through its European Observatory on Infringements of Intellectual Property Rights and CEPOL (the European Union Agency for Law Enforcement Training) jointly organized the training workshop. The workshop was held at the EU police training facility in Paris, France. The aim of the workshop was to (1) provide the participating prosecutors and investigators with presentations about experiences with IP prosecutions in a number of EU Member States as well as in the United States, (2) share best practices on interagency and public-private cooperation, and (3) identify the best investigative measures to combat against counterfeiting and IP crime infringement online. The audience included investigators and prosecutors from 10 EU countries who are responsible for investigating and prosecuting IP crime cases. CCIPS gave presentations on the use of digital evidence in online piracy and counterfeit goods prosecutions and on digital investigative techniques, as well as an Internet investigation simulation.

CCIPS Meeting with Latvian Delegation. In July 2017, CCIPS met with a delegation from the Republic of Latvia to discuss CCIPS' role within the Department as it relates to cyber-crime and intellectual property enforcement. The Latvian delegation consisted of a judge, a prosecutor, and an educator from the Latvian School of Public Administration. Topics discussed included CCIPS' coordination with the USAO community, CHIP AUSAs, domestic and international law enforcement, and policymakers.

OTHER REGIONS

Resistant Legal Advisor Trainings. In February 2017, CCIPS addressed 11 participants based in nine countries—Bangladesh, Ethiopia, Kenya, Mexico, Pakistan, the Philippines, Serbia, Sri Lanka, and Timor-Leste—at the DOJ/OPDAT Resident Legal Advisor ("RLA") School in Washington, DC. CCIPS spoke regarding CCIPS's and DOJ's work on cybercrime, intellectual property, and electronic evidence issues in the U.S. and around the world.

Visit from Chief Justice from The Republic of Trinidad and Tobago. In August 2017, CCIPS met with the Chief Justice from the Republic of Trinidad and Tobago. The presentation at CCIPS covered computer crime policy and prosecution, digital evidence collection, and intellectual property law and prosecutions.

Regional Intellectual Property Rights Training in Barbados. In September 2017, the Brazil IPLEC participated in a regional training in Bridgetown, Barbados. The program focused on counterfeit hard goods and the best practices for using effective tools to increase seizures, as well as how to investigate and prosecute these crimes successfully in a challenging legal environment. Police, prosecutors, and customs officers from Barbados, Antigua and Barbuda, St. Kitts and Nevis, St. Lucia, Guyana, Grenada, Belize, Jamaica, Curacao, Trinidad and Tobago, Bermuda, and Suriname participated.

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 FY2017, CCIPS organized and planned its Eleventh Annual IP Industry and Law Enforcement Meeting held in Washington, D.C, in October 2017. 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, Deputy Attorney General Rod Rosenstein provided keynote remarks, and several senior DOJ and law enforcement officials, including Acting Assistant Attorney General Kenneth Blanco and officials from FBI, ICE-HSI, CBP, and FDA participated in the meeting. Approximately 90 government 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, workshops, and events attended by IP rights holders and law enforcement officials. These events included, among others:

- In October 2016, a DOJ Consumer Protection Branch attorney presented to the Pharmaceutical Security Institute's 30th General Assembly in Cambridge, Massachusetts, on prosecuting counterfeit drug cases. The presentation included means of industry assistance that complement law enforcement investigations and prosecutions.

- In October 2016, CCIPS presented at a roundtable in Charleston, South Carolina for the General Counsel of more than 20 mid-sized law firms (firms with 150-450 lawyers). CCIPS's presentation, entitled "Cybercrime and Intellectual Property Crime: A Team Effort," focused on the importance of lawyers and their clients developing relationships with law enforcement in advance of a cybersecurity or IP theft incident, and contacting law enforcement as soon as possible when an incident does occur.

- In October 2016, CCIPS participated in a panel discussion at the FBI's General Counsel Cyber Summit at University of California Berkeley Law School. The symposium was organized by FBI's Cyber Division, as an outreach opportunity to general counsels of Silicon Valley companies, and included presentations on how cyber investigations are conducted and attendant legal issues that affect law enforcement's ability to conduct them effectively. DOJ contributed content on how cyber intrusions or trade secret theft can be reported and legal issues associated with information sharing, including issues arising under the newly enacted Cybersecurity Act of 2015.

- In October 2016, CCIPS presented at the 15th Annual Law Firm COO & CFO Forum in New York City, New York. CCIPS's presentation, entitled "Cybercrime and IP Crime: A Team Effort." focused on the importance of developing relationships with law enforcement before a cyber or IP incident and of involving law enforcement as soon as an

incident occurs. More than 250 lawyers are expected to attend the Forum at The Thomson Reuters Legal Executive Institute.

- In December 2016, CCIPS participated in the Semiconductor Industry Association's briefing on anti-counterfeiting in Washington, D.C. Industry representatives from Intel and Texas Instruments, among others, met with government representatives from Commerce, DHS, and DOJ to discuss the proliferation and detrimental public impact of counterfeit semiconductor components in the United States and to explore ways to increase international cooperation in combatting the issue.

- In January 2017, CCIPS participated in meetings with Automotive Anti-Counterfeiting Council ("A2C2") representatives; ebay representatives; and FBI, HSI, and USPIS representatives. ebay hosted the meetings at their facility in Draper, Utah. The full-day agenda consisted of A2C2 and USG briefings, presentations by multiple ebay units, and discussions focused on the sales of airbags and other supplementary restraint systems on e-commerce platforms, sharing best practices by industry, and improving ebay's internal scrutiny of listings to limit counterfeits on its platform.

- In January 2017, CCIPS, along with representatives of the FBI and ICE/HSI, met with Facebook representatives to discuss the challenge of reducing the sale of counterfeit, pirated and other fraudulent merchandise in Facebook's recently implemented Marketplace platform. The meeting included discussion of cases arising on other online marketplace systems and best practices in identifying and reporting criminal activity.

- In February 2017, CCIPS met with representatives of the Entertainment Software Association (ESA) to gain insight on the impact of IP and Computer Crime on ESA member companies. ESA presented information about trends in gaming piracy and its internal investigative techniques. CCIPS also made suggestions for best practices for DOJ's future work with industry to investigate, prosecute, and deter these crimes.

- In March 2017 and September 7, 2017, CCIPS and the IPR Center co-hosted half-day meetings 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. Approximately 65 industry, government, and law enforcement representatives attended the meeting.

- In March 2017, CCIPS met with representatives of Liberty Puerto Rico at a meeting hosted by the National Intellectual Property Rights Coordination Center in Arlington, Virginia. At the meeting, counsel for Liberty Puerto Rico discussed the difficulties that Liberty, along with other small-and medium-sized cable providers in the American Cable Association, and a broad range of content owners, is experiencing due to recent growth in unauthorized fee-based streaming services that provide pirated content through "set top" media players.

- In May 2017, CCIPS met with representatives from the Entertainment Software Alliance (ESA) and law enforcement, including HSI and CBP. The National Intellectual Property

Rights Coordination Center in Alexandria, Virginia, hosted the meeting, which focused on intellectual property rights enforcement, including copyright infringement, piracy, and trademark counterfeiting.

- In May 2017, CCIPS attended the spring meeting of the Automotive Aftermarket Suppliers Association (AASA) and the Motor & Equipment Manufacturers Association (MEMA) in Washington, D.C., to discuss intellectual property rights enforcement. AASA and MEMA are trade associations that represent businesses in the automotive aftermarket and motor vehicle suppliers and parts industries, respectively. Other participants included representatives from the USPTO and law enforcement, including the FBI, HSI, and CBP.

- In June 2017, CCIPS participated on a panel at Merck Pharmaceutical's Product Integrity Investigative Summit in Los Angeles, California. The summit serves as Merck's annual global meeting for all Merck Global Security employees who lead or execute investigations and all of their outside investigators and counsel involved in anti-counterfeit investigations, internal investigations, and FCPA compliance. CCIPS's presentation highlighted the need for effective partnerships and coordination among prosecution, law enforcement, and trademark holders in criminal counterfeit investigations, as well as some potential pitfalls.

- In June 2017, CCIPS met with the Recording Industry Association of America, about intellectual property IP issues affecting the recording industry generally as well other domestic and international IP policy issues.

- In June 2017, CCIPS spoke in Los Angeles, CA at the Eighth Annual Anti-Piracy and Content Protection Summit. The summit is a leading event bringing together private sector and government lawyers and managers in the area of intellectual property, content protection, antipiracy, security, and digital rights. In the past few years, many of the nation's largest companies affected by copyright infringement and content theft have participated in the event. CCIPS addressed DOJ's efforts to investigate and prosecute counterfeiting and piracy; working with law enforcement; and emerging enforcement issues.

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.

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.

(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 2017, listing the number of defendants and cases charged, the number of defendants sentenced, and the length of those sentences.[9] 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 2017
Investigative Matters Received by AUSAs	178
Defendants Charged	101

[9] 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.

Cases Charged	77
Defendants Sentenced	70
No Prison Term	42
1-12 Months	12
13-24 Months	3
25-36 Months	4
37-60 Months	6
60 + Months	3

In addition, we have provided the chart below with FY 2017 statistics for criminal IP cases broken down by type of charge.[10]

Charge	Cases charged	Percentage
Trademark *Trafficking in counterfeit goods, 18 U.S.C. § 2320*	56	71%
Copyright *Criminal copyright infringement, 17 U.S.C. §506* *Counterfeit labels, 18 U.S.C. § 2318* *DMCA, 17 U.S.C. § 1201*	 8 2 2	 10% 3% 3%
Economic Espionage Act *Economic espionage, 18 U.S.C. § 1831* *Theft of trade secrets, 18 U.S.C. § 1832*	 2 9	 3% 11%
Total	**79**	**100%**

[10] 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.

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

The Criminal Division currently devotes fifteen 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.

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, 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) and economic espionage investigations. 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 since 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 expanded IPLEC program in FY 2016 by posting new regional IPLECs in Hong Kong and Sao Paolo, Brazil. Most recently, in FY 2017, the State Department and DOJ prepared to field a new IPLEC position in Abuja, Nigeria. The Nigeria IPLEC deployed in October 2017, bringing the total number of regional IPLECs up to five DOJ prosecutors.

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 works closely with the NSCS Network to assist in coordinating national prosecution initiatives designed to counter the national security cyber threat. 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
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 2017 Report to Congress on Intellectual Property Enforcement
FY 2017	Fiscal Year 2017
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

PRC	People's Republic of China
PRO IP Act	*Prioritizing Resources and Organization for Intellectual Property Act of 2008*
USPTO	U.S. Patent and Trademark Office