United States Department of Justice

PRO IP Act
Annual Report FY 2019

PRO IP ACT ANNUAL REPORT OF THE ATTORNEY GENERAL FY 2019

INTRODUCTION

The Department of Justice (the "Department" or "DOJ")[1] submits this Fiscal Year 2019 ("FY 2019") 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 2019 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 2019 (*i.e.*, October 1, 2018 through September 30, 2019) are set forth below.

In addition, working closely with the Office of the Intellectual Property Enforcement Coordinator ("IPEC"), the Department contributed to the FY 2017-2019 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 2019, the Office of Justice Programs ("OJP") awarded grants to support state and local IP law enforcement task forces under statutory authority provided by the Consolidated Appropriations Act, 2019, Public Law No. 116-6, 133 Stat. 13, 113, 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 through training and technical assistance 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 2019, OJP was able to grant six awards totaling $2,254,345 to local and state law enforcement and prosecutorial agencies. The following FY 2019 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
2019-H3269-IL-IP	Cook County State's Attorney's Office	$400,000.00
2019-H3242-CA-IP	City of Los Angeles	$352,000.00
2019-H3235-NC-IP	North Carolina Department of the Secretary of State	$352,000.00
2019-H3250-NJ-IP	Essex County Prosecutor's Office	$350,345.00
2019-H3261-PA-IP	Pennsylvania State Police	$400,000.00
2019-H3252-MO-IP	City of Saint Louis Metropolitan Police Department	$400,000.00

Since the inception of the program, OJP has awarded over $30 million 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 over $23 million. Throughout the duration of the program, these agencies have made seizures totaling over $850 million, which includes counterfeit merchandise and other property as well as currency.

During a one – year period July 1, 2018 – June 30, 2019, grantees reported seizures totaling $179,721,197 ($178,562,461.40 in counterfeit merchandise and other property, and $1,158,735.95 in currency). Over this same one-year period, grantees engaged in the following law enforcement activities:

- 305 individuals were arrested for violations of IP laws;
- 138 state and local IP search warrants were served; and
- 407 piracy/counterfeiting organizations were disrupted or dismantled.

This data comes from the Bureau of Justices Assistance's Performance Measurement Tool (PMT) for recipients of IPEP awards.

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

- The Essex County Prosecutors Office IP Unit/Task Force conducted an investigation in conjunction with the New Jersey Department of the Treasury Division of Taxation Office of Criminal Investigation. The Department of Homeland Security also assisted in this investigation. This investigation targeted numerous individuals and businesses that were suspected of selling smuggled cigarettes into New Jersey with counterfeit New Jersey tax stamps affixed to them. This investigation resulted in the execution of seven search warrants, the arrest of four individuals, the seizure of numerous bank accounts, the seizure of over $100,000.00 is U.S. currency, and the seizure of over 500 counterfeit tax stamps. These charges are pending prosecution in Essex County Superior Court.

- The Virginia State Police had several major accomplishments during this reporting period. The Virginia State Police continues to work with Pfizer on a very large prescription fraud drug ring within Virginia. The Virginia State Police are working several counterfeit credit card cases that have resulted in leads in other states involving the same suspects. These cases are still under investigation. The Virginia State Police also continued to utilize shared databases to work with other agencies to provide intelligence regarding its investigation. The liaison activity established by the Virginia State Police has allowed them to be more specialized in assisting and educating other law enforcement agencies about the fight against intellectual property crimes in Virginia. The agents trained also have conducted training to make civilians and other law enforcement agencies aware of intellectual property crimes. Six agents have attained the status of Certified Fraud Examiner. The Virginia State Police also were able to utilize its funds to purchase equipment and supplies to aid in their investigations.

BJA 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 October 1, 2018 and September 30, 2019, NW3C conducted these training sessions for 212 attendees from 85 agencies in 6 locations. During this time, NW3C also conducted technical assistance for five IPEP Grantee task forces. Additional technical assistance was provided by request to two other law enforcement agencies. NW3C's online IP resource to improve investigative and prosecutorial approaches to the problem of IP theft was utilized by 159 students.

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

- 110 trainings for 2,609 attendees from 1,301 agencies
- 16 seminars for 538 attendees from 185 agencies
- 39 technical assistance visits for 568 attendees from 130 agencies
- 295 students representing 277 agencies have accessed the online IP resource

NW3C launched the website IPTheft.org to provide a common place for IPEP grantees and law enforcement to find training, resources, and technical assistance that will aid in their intellectual property theft investigations. The website also contains legal resources for prosecutors and judges as well as resources for the general public. In the coming year, NW3C plans to promote the website through its communication platforms and grow the site in terms of available training and resources.

Examples of how attendees utilized the training and technical assistance include:

- NW3C instructors performed a technical assistance visit with multiple law enforcement agencies in Louisville, Kentucky. Louisville Metro Police executed a search warrant and seized over $1.5 million worth of counterfeit goods. This was a misdemeanor offense under Kentucky laws. After discussing the penalties imposed for similar offenses in other states with the NW3C instructors, the Kentucky law enforcement officials began pursuing legislative changes to the intellectual property rights statutes in the state of Kentucky to increase the penalties for these types of crimes.

- During a technical assistance visit to the North Carolina Secretary of State's IP task force, an NW3C IP Instructor facilitated collaboration between Homeland Security Investigations agents in Roanoke, Virginia and North Carolina law enforcement officials to investigate intellectual property rights violations discovered at a mailing facility in North Carolina with counterfeit items also going to Western Virginia. These investigations developed evidence of probable cause, leading to multiple search warrants, arrests, and thousands of dollars of counterfeit goods seized, as well as an ongoing collaborative relationship between Virginia and North Carolina to combat intellectual property crime.

(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.

(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 2018, Congress did not appropriate funds to support Section 402(b) of the PRO IP Act in FY 2019.[2] 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 2019, the Department has taken the following additional actions to address this important issue:

[2] Section 402(b) provides that "[s]ubject to the availability of appropriations to carry out this subsection, and not later than 180 days after the date of the enactment of this Act, the Attorney General, through the United States Attorneys' Offices, the Computer Crime and Intellectual Property section, and the Organized Crime and Racketeering section of the Department of Justice, and in consultation with the Federal Bureau of Investigation and other Federal law enforcement agencies, such as the Department of Homeland Security, shall create and implement a comprehensive, long-range plan to investigate and prosecute international organized crime syndicates engaging in or supporting crimes relating to the theft of intellectual property."

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 2019, 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 2009-2013. No funds were appropriated under this section or expended during FY 2019 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 2019.

(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 ("NSD"), 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 not only 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.[3]

The Department made substantial contributions to the criminal enforcement proposals contained in the Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations (March 2011), the majority of which (described above) were enacted into law, with the exception of felony penalties for copyright infringement by online streaming. 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 FY 2017-2019 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;

[3] For an overview of the Department's policies and efforts in the five years prior to the enactment of the PRO IP Act in October 2008, the Department's PRO IP Act First Annual Report 2008-2009 may be found online at https://www.justice.gov/iptf/pro-ip-act-reports. The Department's FY 2010-FY 2018 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 U.S. Transnational and High Tech Crime Global Law Enforcement Network ("GLEN") of regional International Computer Hacking and Intellectual Property ("ICHIP") attorneys (formerly, the Intellectual Property Law Enforcement Coordinator ("IPLEC") program). With the support of the State Department, DOJ has posted ICHIPs in Bucharest, Romania; Hong Kong; Sao Paolo, Brazil; Abuja, Nigeria; Bangkok, Thailand; Kuala Lumpur, Malaysia; and The Hague, Netherlands. The GLEN also now includes two ICHIPs based in Washington, D.C. to assist the regional ICHIP Advisors with the subject matter areas of Global Dark Web and Cryptocurrency issues and Global Internet Based Fraud and Public Health issues, and a Global Cyber Forensic Advisor also based in Washington, D.C. In 2020, the Network will expand to include regional ICHIPs based in Panama City, Panama; Zagreb, Croatia; and Addis Ababa, Ethiopia.

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

CES and the NSCS Network

Within NSD, 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.[5] 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 six 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 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

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

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

national security cybercrimes, and to coordinate and de-conflict national security cyber investigations.

Interagency Coordination

In addition to investigating and prosecuting IP crime, the Department has worked closely with other federal agencies directly, and through the National Intellectual Property Rights Coordination Center ("IPR Center"), to improve IP enforcement domestically and overseas.[6] These activities have included training investigators and prosecutors in the investigation and prosecution of IP crimes; contributing to the Office of the United States Trade Representative's Special 301 process of evaluating the adequacy of our trading partners' criminal IP laws and enforcement regimes; helping to catalogue and review the United States government's IP training programs abroad; and implementing an aggressive international program to promote cooperative enforcement efforts with our trading partners and to improve substantive laws and enforcement regimes in other countries.

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

The Department achieved notable success in FY 2019 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

[6] 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, the Federal Maritime Commission, and the Department of Veterans Affairs Office of Inspector General.

military goods. In FY 2019, this initiative resulted in a number of significant prosecutions, including those set forth below:

- *San Francisco Resident Sentenced to 10 Years in Prison for Manufacturing Counterfeit Adderall Pills Containing Methamphetamine.* On November 27, 2018, Gino Carl von Eckstein, of Brisbane, California, was sentenced to 10 years in prison for possessing with intent to distribute methamphetamine. Eckstein pleaded guilty on September 5, 2018. He admitted that he possessed counterfeit "Adderall" pills, or pills that appeared to be Adderall, but in fact contained methamphetamine. Eckstein admitted he stored the pills in his car, at three locations in San Francisco's Richmond District, in Brisbane, and in San Leandro. Eckstein further admitted he possessed the equipment and ingredients necessary to manufacture counterfeit Adderall pills. In total, agents allegedly found over 1,000 grams of suspected methamphetamine.

- *Stamford Men Charged with Trafficking Counterfeit Oxycodone Pills Containing Fentanyl Analogues.* On April 24, 2019, an indictment was unsealed charging Vincent Decaro, Arber Isaku, and David Reichard, all of Stamford, Connecticut, with offenses related to the trafficking of fentanyl analogues. Decaro and Isaku purchased fentanyl analogues from suppliers in China and, working out of Decaro's residence at 77 West Hill Circle in Stamford, pressed the drug into counterfeit oxycodone pills, which they sold to customers on dark web markets. Reichard was arrested on a federal criminal complaint on April 13, 2018. He previously entered a plea of not guilty to the charges in the indictment.

- *Champaign Man Pleaded Guilty to Charges for Trafficking Counterfeit Xanax, Money Laundering.* On April 29, 2019, Stephan Caamano, of Champaign, Illinois, entered guilty pleas to charges that he trafficked quantities of pills containing alprazolam, marked as 'Xanax,' and laundered proceeds of the alleged drug trafficking. The superseding indictment returned by the grand jury on October 2, 2018 alleged that from March 2017 to May 2018, Caamano trafficked quantities of pills containing alprazolam, marked as 'Xanax,' knowing it was not the drug Xanax manufactured by Pfizer. In addition, Caamano was charged with two counts of distribution of alprazolam, a Schedule IV controlled substance, and four counts of money laundering related to monetary transactions involving proceeds of the alleged drug trafficking. The charged money laundering transactions involved payment of Bitcoin in exchange for gold bullion on two occasions - April 12, 2017 and June 9, 2017; a wire transfer in the amount of $235,500 on or about July 31, 2017; and, the transfer of funds on August 30, 2017, by personal check to a car dealership in the amount of $25,936. Caamano's sentencing hearing is scheduled for January 6, 2020.

- *Two Mexican Nationals Indicted for Transporting Approximately 14,800 Counterfeit Oxycodone Pills Containing Fentanyl.* On May 23, 2019, a two-count indictment against Ivan Lopez, of Mexico, and Erick Olivas Lopez, of Mexico, charged them with conspiracy and possession with intent to distribute at least 400 grams of a substance

containing fentanyl. According to court documents, on April 25, 2019, the defendants were found in possession of approximately 14,799 fentanyl-laced counterfeit oxycodone pills, weighing approximately 1.6 kilograms, during a traffic stop in Sacramento.

- *Long Beach Man Sentenced to Almost Four Years in Prison for Trafficking Counterfeit Prescription Drugs.* On May 24, 2019, Robert Ashton Kerns, of Long Beach, Mississippi, was sentenced to 46 months in federal prison, followed by 3 years of supervised release, for possession with intent to distribute fentanyl and fentanyl analogues. On June 12, 2018, Kerns was charged in a federal criminal indictment. He pled guilty on March 1, 2019 to one count of possession with intent to distribute fentanyl and fentanyl analogues.

- *Two Sentenced for Buying and Selling Counterfeit Airbags.* On May 9, 2019, Raymond Whelan was sentenced to serve 24 months in prison for conspiracy to traffic in air bags. On May 28, 2019, his codefendant, David Nichols, was sentenced to serve 12 months in prison for conspiracy to traffic in counterfeit air bags. Both defendants also were ordered to pay $75,846 in restitution. According to charging documents filed in the Western District of New York, between June 2015 and March 2016, Whelan, of Cheektowaga, New York and Nichols of Marysville, Ohio, imported and sold counterfeit automobile air bags from China. Whelan contacted Nichols and ordered numerous airbags bearing counterfeit trademarks of Honda, Toyota, Nissan, Subaru, Mazda, Hyundai, Acura, and Mitsubishi. Nichols then located manufacturers in China to supply the requested airbags. In order to avoid detection during importation, the airbags were purposefully mislabeled. Once imported into the United States, Whelan sold the airbags as genuine used airbags on eBay utilizing the name Rayscarparts71. Whelan imported and sold approximately 360 counterfeit automobile airbags, with an average manufacturer's retail price of $650.00. The total infringement amount was $236,600. Nichols entered a plea of guilty in January of 2018. Whelan entered a plea of guilty in August of 2018.

- *Large-Scale Counterfeit Fentanyl Pill Dealer Convicted at Trial.* On June 5, 2019, Dion Gregory Fisher, formerly of Seminole, Florida, was found guilty of conspiring to manufacture and distribute fentanyl and fentanyl analogue, and money laundering. In addition to the conspiracy count, the jury found Fisher guilty of five counts of fentanyl distribution and manufacturing and eight counts of committing money laundering transactions involving more than $10,000 of narcotics proceeds. Fisher was charged with his co-defendant, Sam Huffman, who had used the pill presses and materials provided by Fisher to press fentanyl pills at his automotive business in Pinellas Park, Florida. Fisher also stored fentanyl and fentanyl analogue in a work bay in Clearwater. In January and February 2018, large quantities of fentanyl and fentanyl analogue were seized from both locations, as well as from Fisher's residence in Seminole, and McKinney's residence and work bay. More than three kilograms of fentanyl and fentanyl analogue were admitted into evidence during the seven-day trial. Fisher laundered the proceeds from his fentanyl pill sales with Konrad Guzewicz, who owned and operated automotive and tire-and-rim companies in Pinellas County. Fisher purchased several high-end luxury vehicles, including an Aston Martin, a Bentley, a Maserati, a BMW, and an Audi R8, with fentanyl proceeds. Guzewicz also laundered fentanyl cash proceeds for Fisher. On four occasions,

Fisher provided Guzewicz with $35,000 in cash he had obtained from selling fentanyl pills, and Guzewicz in turn wrote Fisher a $30,000 check from his business and personal accounts. On October 31, 2019, Fisher was sentenced to 30 years in federal prison, and on July 2, 2019, Guzewicz was sentenced to 15 months in federal prison.

- *Wholesaler Admits to Conspiracy to Manufacture and Sell Counterfeit Goods to the U.S. Military & Government.* On June 13, 2019, Ramin Kohanbash, pleaded guilty to conspiracy to commit wire fraud and trafficking in counterfeit goods in the District of Rhode Island. Kohanbash and others had arranged to counterfeit 200 military parkas of a type used by U.S. Air Force personnel stationed in Afghanistan. These parkas were falsely represented to be genuine Multicam®, a fabric which incorporates specialized near-infrared management technology designed to make the wearer more difficult to detect with equipment such as night-vision goggles. The goods were shipped from China to Kohanbash and sold to other wholesalers who ultimately marketed and sold the knock-off products to military and government buyers as genuine, American-made products. In order to sell the counterfeit goods, Kohanbash provided wholesalers who did business with the government with false certification letters claiming that the goods were made in the U.S., and therefore complied with the Berry Amendment. In other instances, Kohanbash falsely represented that the goods met Trade Agreement Act requirements.

- *Dominican National Sentenced for Fentanyl Conspiracy Including the Distribution of Counterfeit Pain Pills.* On July 11, 2019, Santiago Pena was sentenced to serve 24 months in prison for his role in a conspiracy to distribute fentanyl. On December 20, 2017, Pena was charged with conspiracy to distribute 40 grams or more of fentanyl. The charge stemmed from Pena's participation in a large-scale fentanyl and heroin trafficking ring that was dismantled in August 2017. Pena was the seventh defendant related to the drug trafficking operation to be charged in federal court; approximately 10 other defendants were charged in state court. A lengthy wiretap investigation revealed that James Ramirez, an individual charged separately, supplied large-quantities of fentanyl and heroin to drug dealers on Cape Cod. According to the indictment, Pena brokered fentanyl pill deals on Ramirez's behalf, helping to connect Ramirez with a fentanyl pill supplier. Pena pleaded guilty on March 19, 2018.

- *Two Mexican Nationals Sentenced to Five Years' Probation for Trafficking in Counterfeit Goods by Operating Counterfeit Airbag Business in Albuquerque*. On August 13, 2019, two Mexican nationals were sentenced to serve five years each for operating a counterfeit airbag business out of their residence in Albuquerque, New Mexico. Dina Gonzalez-Marquez and Emilio Gonzalez-Marquez were indicted in April of 2017 on charges that they conspired to traffic in counterfeit goods from January 2015 to March 2017, by operating a business that sold counterfeit airbag modules and airbag covers out of their Albuquerque residence. According to the indictment, they facilitated the conspiracy by listing and selling counterfeit airbag modules and airbag covers online, shipping the counterfeit goods to purchasers, and conducting in-person sales of the counterfeit goods.

- *Orange County Man Sentenced to 17½ Years in Federal Prison for Selling Counterfeit Opioid Pills Laced with Fentanyl.* On August 26, 2019, Wyatt Pasek, of Santa Ana, California, who admitted his role in a scheme that used fentanyl and other synthetic opioids to manufacture and sell counterfeit pharmaceutical pills designed to look like brand-name oxycodone pills, was sentenced to 210 months in federal prison. Pasek used the moniker "oxygod" when soliciting customers in online marketplaces, and posted images and videos of himself to social media platforms under the moniker Yung10x. He pleaded guilty in November of 2018 to participating in a narcotics-trafficking conspiracy, being a convicted felon in possession of a firearm, and money laundering. On August 29, 2019, Pasek filed an appeal on his final judgement to U.S. Court of Appeals for the Ninth Circuit.

- *Lead Defendant Admits Trafficking in Counterfeit Goods.* On September 10, 2019, Carlos Enrique Velázquez-Gines pleaded guilty to three counts of trafficking in counterfeit goods. On March 7, 2018, Velázquez-Gines, Mayra Evelise Gines-Otero, Noriam Ivette Flores-Deleon, and Vanessa Marrero-Hernández, were charged in the District of Puerto Rico with mail and wire fraud conspiracy, mail fraud, trafficking in counterfeit goods, introducing misbranded articles into interstate commerce, distribution of a controlled substance, international money laundering, and smuggling. According to the indictment, from at least on or about October 3, 2013, defendants purchased from overseas suppliers located in China, and imported into the United States, dietary supplements, latex condoms, and cosmetics that were counterfeit and/or misbranded under the Federal Food, Drug, and Cosmetic Act. Defendants marketed and sold the products through "online stores" on platforms such as eBay.com and Bonanzo.com. Marrero-Hernández pleaded guilty on October 2, 2018, and Flores-Deleon pleaded guilty on October 18, 2018.

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

In FY 2019, 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:

- *Third Defendant Pleads Guilty in Case Charging a Theft of Trade Secrets from GlaxoSmithKline to Benefit Chinese Pharmaceutical Company.* On October 22, 2018, Tian Xue pleaded guilty to a conspiracy to commit money laundering involving the proceeds of a scheme to steal trade secrets from GlaxoSmithKline ("GSK") for the benefit of a Chinese pharmaceutical company named Renopharma. According to an indictment returned in May of 2017, Dr. Tao Li and two of his friends, Dr. Yu Xue and Dr. Yan Mei, created Renopharma in Nanjing, China, supposedly to research and develop anti-cancer drugs. In reality, Renopharma was used as a repository of stolen information from GSK. The data contained information regarding multiple biopharmaceutical products under development, GSK research data, and GSK processes regarding the research, development, and manufacturing of biopharmaceutical products. On January 5,

2016, the FBI arrested Li and seized his computer on which they found a number of GSK documents containing trade secret and confidential information which he had received from Dr. Yu Xue. Dr. Yu Xue pleaded guilty on August 31, 2018 to a conspiracy to steal trade secrets. Dr. Tao Li pleaded guilty on September 17, 2018 to a conspiracy to steal trade secrets. Charges against Dr. Yan Mei and his spouse, Lucy Xi, are still pending.

- *Former Genentech Employees Charged With Theft Of Trade Secrets.* On October 25, 2018, Xanthe Lam, Allen Lam, John Chan, and James Quach were indicted in the Northern District of California for stealing trade secrets from Genentech and related charges. The indictment alleges that the defendants stole confidential Genentech information to help a company in Taiwan create and sell drugs similar to those that were created by Genentech. Xanthe Lam also allegedly secretly consulted for JHL while still employed at Genentech. The indictment also alleges that Xanthe Lam conspired with former Genentech employee James Quach to illegally use her computer credentials. Specifically, she allowed Quach to gain access to Genentech's secure document repository and, once he had access to the repository, Quach stole the company's proprietary manufacturing protocols.

- *PRC State-Owned Company, Taiwan Company, and Three Individuals Charged with Economic Espionage.* On November 1, 2018, an indictment in the Northern District of California was unsealed charging a state-owned enterprise of the People's Republic of China (PRC) with crimes related to a conspiracy to steal, convey, and possess stolen trade secrets of an American semiconductor company for the benefit of a company controlled by the PRC government. All of the defendants are charged with a conspiracy to commit economic espionage, among other crimes. The criminal defendants are United Microelectronics Corporation ("UMC"), a Taiwan semiconductor foundry; Fujian Jinhua Integrated Circuit, Co., Ltd. ("Jinhua'"), a state-owned enterprise of the PRC; and three Taiwan nationals: Chen Zhengkun, a.k.a. Stephen Chen, He Jianting, a.k.a. J.T. Ho; and Wang Yungming, a.k.a. Kenny Wang.

- *Chinese National Who Stole Trade Secrets while Working for Medical Device Companies Sentenced to Federal Prison.* On January 28, 2019, Wenfeng Lu, an Irvine, California engineer who stole trade secrets belonging to two former employers, both of which develop and manufacture medical devices used to treat cardiac and vascular ailments, was sentenced to 27 months in federal prison. Lu pleaded guilty in May 2018 to six counts of unauthorized possession and attempted possession of trade secrets. Lu admitted that he stole confidential and proprietary trade secrets from two different medical device companies with research facilities in Irvine, where Lu worked from January 2009 until he was arrested in this case in 2012. According to court documents, while he was working for the companies, Lu travelled to the People's Republic of China (PRC) multiple times – sometimes soon after stealing the trade secrets from his employers. Lu was arrested as he prepared to board a plane to the PRC in November 2012, which prevented him from

implementing his business plan and causing significant harm to the victim companies in the United States.

- *Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice.* On January 28, 2019, a 10-count indictment in the Western District of Washington was unsealed charging Huawei Device Co., Ltd. and Huawei Device Co. USA with theft of trade secrets conspiracy, attempted theft of trade secrets, seven counts of wire fraud, and one count of obstruction of justice. The indictment details Huawei's efforts to steal trade secrets from Bellevue, Washington based T-Mobile USA and then obstruct justice when T-Mobile threatened to sue Huawei in U.S. District Court in Seattle. As emails obtained in the course of the investigation reveal, the conspiracy to steal secrets from T-Mobile was a company-wide effort involving many engineers and employees within the two charged companies. As part of its investigation, FBI obtained emails revealing that in July 2013, Huawei offered bonuses to employees based on the value of information they stole from other companies around the world, and provided to Huawei via an encrypted email address.

- *One American and One Chinese National Indicted in Tennessee for Conspiracy to Commit Theft of Trade Secrets and Wire Fraud.* On February 12, 2019, Xiaorong You, a/k/a Shannon You, of Lansing, Michigan, and Liu Xiangchen, of Shandong Province, China, were indicted for conspiracy to steal trade secrets related to formulations for bisphenol-A-free (BPA-free) coatings. You was also indicted on seven counts of theft of trade secrets and one count of wire fraud. The BPA-free trade secrets allegedly stolen by these individuals belonged to multiple owners and cost an estimated total of at least $119,600,000 to develop.

- *Former DuPont Employee Sentenced to 42 Months in Prison for Stealing Trade Secrets and Lying to the FBI.* On April 17, 2019, Josh Harry Isler was sentenced to serve 42 months imprisonment for one count of trade secret theft and one count of making a false statement or representation to the FBI. As part of his guilty plea in July of 2018, Isler admitted that during August 2013, while employed with DuPont, but after having accepted an offer of employment from a competitor, he stole trade secrets of DuPont. In a plea agreement, Isler admitted that after he accepted employment with a competitor of DuPont in the ethanol fuel enzyme business, he transferred hundreds of DuPont's electronic files to an external device. Isler also admitted that when he was interviewed by the FBI in November 2013, he falsely denied he had downloaded files containing proprietary information.

- *Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets.* On April 23, 2019, an indictment in the Northern District of New York was unsealed charging Xiaoqing Zheng, of Niskayuna, New York, and Zhaoxi Zhang, of Liaoning Province, China, with economic espionage and conspiring to steal General Electric's (GE's) trade secrets surrounding turbine technologies, knowing and intending that those stolen trade secrets would be used to benefit the People's Republic of China. According to the 14-count indictment, Zheng, while employed at GE Power &

Water in Schenectady, New York as an engineer specializing in sealing technology, exploited his access to GE's files by stealing multiple electronic files, including proprietary files involving design models, engineering drawings, configuration files, and material specifications having to do with various components and testing systems associated with GE gas and steam turbines. The defendants, through LTAT and NTAT, received financial and other support from the Chinese government and coordinated with Chinese government officials to enter into research agreements with Chinese state-owned institutions to develop turbine technologies.

- *Three Indicted for Conspiracy to Steal Trade Secrets from Aircraft Companies.* On May 8, 2019, Gilbert Basaldua, Joseph Pascua, and Craig German were indicted for Conspiracy to Steal Trade Secrets, while Basaldua also has been indicted for Interstate Transportation of Stolen Property. The indictment alleged that all three men agreed to work on developing a product for a competitor company in return for a share of profits. In order to obtain FAA certification for the product, however, an icing wind tunnel testing plan needed to be developed. To shortcut the process of developing this plan, the indictment alleged that all three men agreed to steal trade secrets, including aircraft wing schematics and anti-ice testing documents, from aircraft companies in and outside of the Southern District of Georgia. On September 12, 2019, Craig German pleaded guilty to Conspiracy to Steal Trade Secrets. On November 7, 2019, a superseding indictment was returned adding a fourth defendant, Juan Martinez, to the charge of Conspiracy to Steal Trade Secrets.

- *Massachusetts Man and Semiconductor Company Indicted for Theft of Trade Secrets.* On June 14, 2019, an indictment was unsealed charging Haoyang Yu, a Chinese born naturalized U.S. citizen living in Lexington, Massachusetts, and a company, Tricon MMIC LLC, that Yu and his wife had established, in connection with stealing proprietary information from Yu's former employer, Analog Devices, Inc. (ADI), a semiconductor company headquartered in Norwood, Massachusetts. Yu was indicted on four counts of theft of trade secrets; four counts of copying, uploading, downloading, and attempted copying, uploading, and downloading of a trade secret; four counts of possession and attempted possession of a trade secret; and three counts of smuggling. Tricon MMIC LLC was also indicted on three counts of smuggling.

- *Federal Indictment Charges Software Engineer with Theft of Trade Secrets.* On July 10, 2019, an indictment returned in the Northern District of Illinois was unsealed charging a software engineer at a suburban Chicago locomotive manufacturer who stole proprietary information from the company and took it to China. Xudong Yao, also known as "William Yao," was charged with nine counts of theft of trade secrets. Yao has not yet been arrested. He is believed to be residing in China.

- *Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets.* On July 29, 2019, following a nine-day trial, Shan Shi, of Houston, Texas, was convicted of one count of conspiracy to commit theft of trade secrets. Shi originally was indicted in June 2017 for conspiracy to commit theft of trade secrets. A superseding indictment returned in April of 2018 added one count of conspiracy to commit economic espionage and one count of

conspiracy to commit money laundering. Shi was acquitted on the latter two charges. Evidence introduced at trial established that Shi conspired with others to steal trade secrets from a Houston-based company, Trelleborg Offshore US, Inc., relating to syntactic foam, a strong, lightweight material with commercial and military uses that is essential for deep-sea oil and gas drilling. Four of Shi's codefendants—some of whom worked at Trelleborg —had pleaded guilty to conspiring to steal trade secrets, and two testified as cooperating witnesses at trial. Shi sought to obtain information about syntactic foam for the benefit of CBM-Future New Material Science and Technology Co. Ltd. (CBMF), a Chinese company based in Taizhou, and for the ultimate benefit of the People's Republic of China. From 2014 to 2017, CBMF sent Shi's company in Houston approximately $3.1 million from China in order to promote Shi's activity in the United States.

- *Former Uber Self-Driving Car Executive Indicted for Alleged Theft of Trade Secrets from Google.* Anthony Scott Levandowski of Marin County, California has been indicted on theft of trade secrets charges. The indictment was returned on August 15, 2019, and unsealed on August 26, 2019. The indictment alleges that Levandowski was a Google engineer and one of the founding members of the group that worked on Google's self-driving car project. Levandowski worked on the project from 2009 until he resigned from Google without notice on January 27, 2016. The indictment charges Levandowski with 33 counts of theft and attempted theft of trade secrets.

- *Russian and Italian Nationals Charged with Conspiring to Steal Trade Secrets From American Aviation Company.* On September 5, 2019, a criminal complaint was unsealed in the Southern District of Ohio, charging a Russian national and an Italian national with conspiring and attempting to steal trade secrets from an American aviation company. Alexander Yuryevich Korshunov, and Maurizio Paolo Bianchi, were charged by a criminal complaint on August 21, 2019. Korshunov was arrested on August 30, 2019 at Naples International Airport in Italy.

(3) Large-Scale Commercial Counterfeiting and Online Piracy

The Department continues to pursue significant, large-scale piracy and counterfeiting operations. In FY 2019, the Department has had a number of significant prosecutions, including those set forth below:

- *California Man Sentenced for Copyright Infringement.* On October 15, 2018, Craig M. Vincent, of Stockton, California, was sentenced to serve three years on federal probation for unlawfully selling copyrighted aviation data updates. On July 23, 2018, Vincent pleaded guilty in the District of Kansas to one count of criminal infringement of a copyright. In his plea, Vincent admitted he used eBay to resell aviation navigational database updates in violation of Jeppesen Company's licensing agreement for a trademarked product called NavData. Jeppesen is a Boeing subsidiary. Jeppesen's NavData includes airport information, runway characteristics, waypoints, arrival routes, departure routes, terminal procedures and general information that a Global Positioning System or flight management computer needs to navigate an airplane to final destination.

Jeppesen sold NavData subscriptions to Kansas-based Garmin, Inc. Garmin received a commission from the sales of Jeppesen data sets. Doing business as Merlin Enterprises, Vincent sold NavData cards and required customers to return old data cards to him.

- *New York Woman Sentenced for Trafficking Over $3 Million In Counterfeit Footwear And Handbags Through Port Of Newark.* On October 22, 2018, Xiao Xia Zhao, was sentenced to 18 months imprisonment and three years of supervised release. Zhao had pleaded guilty, on May 23, 2018, to trafficking in counterfeit goods. In total, Zhao trafficked in thousands of pairs of fake Nike footwear, Louis Vuitton handbags, and other counterfeit items, with a total estimated retail value of over $3 million. Zhao also paid individuals over $75,000 in exchange for the delivery of the containers.

- *Queens Resident Sentenced to 30 Months' Imprisonment for Smuggling Counterfeit Apparel into the United States from China.* On November 2, 2018, Su Ming Ling, a resident of Queens, New York, was sentenced to 30 months' imprisonment and ordered to pay $12,905.67 in restitution for one count of fraudulent importation and transportation of goods and one count of conspiracy to traffic in counterfeit goods. The charges arose out of Ling's participation in a scheme to import more than 200 shipping containers of counterfeit brand-name apparel from the People's Republic of China. In aggregate, the counterfeit apparel imported by the defendant and his co-conspirators between May 2013 and January 2017, if sold in the United States as genuine, would have retailed for an estimated $297 million. Ling pleaded guilty to the charge on January 5, 2018. The 211 shipping containers Ling smuggled into the United States included counterfeit goods, such as Nike shoes, UGG boots and NFL jerseys. Ling also hired CBP-licensed customs brokers to file customs entry forms on behalf of the businesses whose identities he had stolen and provided those customs brokers with falsified shipping documents. The counterfeit goods were distributed to locations in Brooklyn, Queens and New Jersey, among other areas.

- *Three Puerto Rican Men Arrested on Federal Charges in Dish Network Services Piracy Scheme.* On November 2, 2018, an indictment was unsealed charging three Puerto Rican men after their arrest for their roles in a conspiracy to provide pirated DISH Network (DISH) services to thousands of Puerto Ricans. The three-count indictment charges Arnaldo Vazquez, aka "Naldo," aka "naldo.dish;" Awildo Jimenez, aka "Wildo," "joselo626," and "wildo20;" and Higinio Lamboy, aka "Ingi," with one count of conspiracy to circumvent protective systems, infringe copyrights and traffic in satellite decryption devices, one substantive count of trafficking in technology designed to circumvent technology copyright protection systems and one substantive count of circumventing a technological measure that protects a copyrighted work. The indictment alleges that the defendants used online chat forums to discuss their criminal enterprise, resolve technical problems related to their DISH piracy, and facilitate the payment for their criminal deeds and purchase of equipment needed to further their scheme.

- *Members of International Movie Piracy Ring Indicted in Scheme to Steal and Sell Pre-Release Hollywood Films and TV Shows.* On December 12, 2018, five men in four countries were charged alleging they distributed or offered for sale stolen digital versions

of hundreds of motion pictures and television shows – including "Fifty Shades of Grey," "The Expendables 3," and "The Walking Dead" – prior to their official release. The charged defendants are: Malik Luqman Farooq, a resident of the United Kingdom; Aditya Raj, believed to reside in India; Sam Nhance, believed to reside in Dubai, United Arab Emirates; Ghobhirajah Selvarajah, believed to reside in Malaysia, and; Jitesh Jadhav, also believed to reside in India. The defendants used a shared PayPal account to receive and distribute money from the sale of the pirated motion pictures, the indictment states. In February 2015, one of the defendants allegedly told a prospective buyer that the ring would be offering copies of the films "Kingsman: The Secret Service" and "Fifty Shades of Grey" for sale on the same day as their U.S. theatrical release. The co-conspirators are also alleged to have previously operated a website used to distribute pirated "Bollywood" films, known as "BollyTNT.".

- *Chinese National Sentenced for Selling Counterfeit Computer Parts.* On February 15, 2019, Ruiyang Li, a Beijing, China, man was sentenced to federal prison for directing the shipment of counterfeit computer-networking equipment into the Southern District of Texas. Li was sentenced to serve 54 months in federal prison. The court also ordered restitution to the victims of Li's trademark counterfeiting—including $812,000 to Cisco Systems Inc., $2,170,000 to the Hewlett-Packard Company and $12,955.91 to Intel Corporation. Because Li is not a U.S. citizen, he is expected to face deportation proceedings after serving his prison sentence. Because counterfeit parts are often not subject to stringent manufacturing requirements, they present a significant health and safety risk to communities across the United States.

- *United States Files Complaint Seeking Forfeiture of Thousands of "Fashion Dolls" That Infringe on Mattel's "Barbie" Copyright.* On April 25, 2019, it was announced that a civil forfeiture complaint was filed seeking to forfeit and recover approximately 21,852 fashion dolls that infringe a registered copyright owned by Mattel, Inc. According to the forfeiture complaint, the importer, Greenbrier International Inc. d/b/a Dollar Tree Inc., and Dollar Tree Distribution ("Greenbrier") listed the contents of the shipping container as "Other Toys" on its manifest. Representatives of Mattel reviewed photographs of the fashion dolls and confirmed that they were unauthorized copies that infringed the "CEO Barbie" doll head copyright owned by Mattel, Inc. As alleged in the forfeiture complaint, in 2016, Greenbrier attempted to import 13,296 Mermaid fashion dolls that were seized at the border by CBP for infringement of the CEO Barbie head sculpt. In both instances, the counterfeit dolls originated from the same exporter/shipper located in Hong Kong.

- *Three Individuals Indicted in Conspiracy to Sell Counterfeit Apparel and Accessories.* On June 6, 2019, Zi Yu Zheng, Xiao Ling Wei, and Ling Wu Wei, all from Maryland, were indicted for trafficking in counterfeit goods through their operation of a retail store and warehouse used to sell apparel and accessories under unauthorized trademarks. The indictment alleges that the three individuals openly displayed the counterfeit merchandise in the retail store, while engaging in various security and counter-surveillance measures to prevent detection by law enforcement, including limiting access to their warehouse to individuals and customers they knew, prohibiting cell phones in the warehouse, and maintaining a secret showroom of counterfeit merchandise behind a false emergency

door. According to the indictment, law enforcement penetrated the conspiracy through controlled purchases executed by confidential sources and an undercover agent.

- *New Orleans Man Sentenced To 3 Years' Probation after Previously Pleading Guilty To Trafficking In $193,980 Worth of Counterfeit Goods.* On June 25, 2019, Maher Salim, age a resident of New Orleans, Louisiana, was sentenced to three years of probation after previously pleading guilty to trafficking in counterfeit goods, on February 12, 2019. According to court documents, Salim owned and operated BRANDS 4 LESS, a business located at 4200 Washington Avenue, Unit A, in New Orleans. During the search, agents seized numerous counterfeit goods Salim was selling that bore the false marks of makers of clothing and luxury goods, including True Religion, Rock Revival, Michael Kors, Coach, Louis Vuitton, Polo, Timberland, New Era, Nike, Adidas, Dolce & Gabbana, Mitchell & Ness, and North Face. The collective fair market value of all the items was approximately $193,980.

- *Florida Attorney Sentenced to 60 Months in Prison for Multi-Million Dollar Pornography Film Copyright Fraud Scheme.* On July 9, 2019, John L. Steele, a Florida attorney was sentenced to 60 months in prison followed by two years of supervised release for his role in a multi-million dollar fraud scheme to obtain payments from extortion victims to settle sham copyright infringement lawsuits by lying to state and federal courts throughout the country. Steele, who pleaded guilty on March 6, 2017, was also ordered to pay restitution in the amount of $1,541,527.37. According to his guilty plea and documents filed in court, between 2011 and 2014, Steele and his co-defendant Paul R. Hansmeier, both practicing lawyers, executed a scheme to obtain millions of dollars by threatening copyright lawsuits against individuals who allegedly downloaded pornographic movies from file-sharing websites. In total, Steele and Hansmeier obtained approximately $3 million from the fraudulent copyright lawsuits.

- *Chinese National Sentenced to Over Three Years in Prison for Trafficking Counterfeit Apple Goods into the United States.* On July 30, 2019, a Chinese national living in the United States on a student visa was sentenced to 37 months in prison followed by one year of supervised release for his role in a scheme to traffic and smuggle counterfeit Apple products, including phony iPhones and iPads, from China into the United States. Jianhua "Jeff" Li, previously pleaded guilty in the District of New Jersey to one count of conspiracy to traffic in counterfeit goods and labels and smuggle goods into the United States and one count of trafficking in counterfeit goods. Over $1.1 million in sales proceeds were wired from U.S. accounts into accounts Li controlled overseas. LaMarca, Becerra, and Volpe previously pleaded guilty to their respective roles in the scheme. LaMarca was sentenced July 21, 2017, to serve 37 months in prison. Becerra and Volpe were sentenced Oct. 15, 2018, to serve three years' probation and 22 months in prison, respectively.

- *Eight Defendants Charged with Running Two of the Biggest Illegal Television Show And Movie Streaming Sites in the United States.* On August 27, 2019 a federal grand jury indicted eight defendants—Kristopher Lee Dallmann, Darryl Julius Polo a/k/a djppimp, Douglas M. Courson, Felipe Garcia, Jared Edward Jaurequi a/k/a Jared Edwards, Peter H.

Huber, Yoany Vaillant a/k/a Yoany Vaillant Fajardo, and Luis Angel Villarino—for conspiracy to commit criminal copyright infringement. In addition, the grand jury charged Dallmann and Polo each with two counts of criminal copyright infringement by reproduction or distribution, two counts of criminal copyright infringement by public performance, and four counts of money laundering, and Polo with two additional counts of criminal copyright infringement by distributing a copyrighted work being prepared for commercial distribution. The eight defendants ran a site called Jetflicks, an online, subscription-based service headquartered in Las Vegas, Nevada that permitted users to stream and, at times, download copyrighted TV programs without the permission of the relevant copyright owners. On December 12, 2019, Polo pleaded guilty to multiple criminal copyright and money laundering charges, and on December 13, 2019, Villarino pleaded guilty to one count of conspiracy to commit copyright infringement.

- *Five Defendants Plead Guilty in Manhattan Federal Court to Multimillion-Dollar Counterfeiting Scheme.* On October 4, 2019, the last of five defendants pleaded guilty to a counterfeit goods conspiracy. On August 7, 2018, defendants Miyuki Suen, Jian Min Huang, Kin Lui Chen, Songhua Qu, and Fangrang Qu were arrested on charges of importing hundreds of thousands of athletic shoes from China into the United States. The defendants are each charged with one count of conspiring to traffic in counterfeit goods, and one count of trafficking in counterfeit goods. From at least in or about January 2016 up to and including in or about July 2018, the defendants imported at least 42 shipping containers holding an estimated more than 380,000 pairs of sneakers from China. Once these shoes arrived, the defendants added trademarked logos to the shoes, rendering them counterfeit. The estimated loss attributable to the defendants' efforts amounts to more than $70 million. All five defendants entered pleas of guilty to the conspiracy count; Fangrang Qu on August 30, 2019; Suen on September 19, 2019; Songhua Qu on September 20, 2019; Huang on September 24, 2019; and Chen on October 4, 2019.

- *Fifteen Defendants Plead Guilty in Scheme to Smuggle Millions of Dollars of Counterfeit Luxury Goods From China Into the United States*. As of December 2019, fifteen defendants charged with smuggling millions of dollars in counterfeit luxury goods pleaded guilty in federal court. On August 16, 2018, six indictments and one criminal complaint were unsealed in federal court, charging a total of 22 defendants with illegally bringing into the United States millions of dollars of Chinese-manufactured goods by smuggling them through ports of entry on the East and West Coasts. All twenty-two defendants were arrested on charges, including conspiracy to traffic, and trafficking, in counterfeit goods; conspiracy to smuggle, and smuggling, counterfeit goods into the United States; money laundering conspiracy; immigration fraud and unlawful procurement of naturalization. The defendants played various roles in the trafficking of counterfeit goods manufactured in China, brought by ocean-going ships to the United States in 40-foot shipping containers, smuggled through ports of entry disguised as legitimate imports and distributed throughout the country. The counterfeit goods included items such as fake Louis Vuitton and Tory Burch handbags, Michael Kors wallets, Hermes belts and Chanel perfume. An additional eleven defendants were referred to the Queen's County District Attorney's Office for prosecution and were convicted in state court of related offenses.

Domestic Training

During the past fiscal 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 2018, CCIPS presented at an Intellectual Property and Trade Enforcement Investigations course at the IPR Center in Arlington, Virginia, to approximately 30 HSI and CBP agents. The presentation covered relevant law and policy, provided practical guidance in counterfeit trademark investigations, and included a case study of U.S. v. Peter Picone, in which a defendant was convicted of selling counterfeit integrated circuits to the U.S. Navy for use in a nuclear submarine.

- In October 2018, NSD, with support from CCIPS, organized and led the annual NSCS Training in McLean, Virginia. 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 November 2018, CCIPS presented at a webinar arranged by and held at the U.S. Patent and Trademark Office for state prosecutors with the National District Attorneys Association (NDAA). The webinar provided an overview of criminal intellectual property laws, and CCIPS presented on best practices for criminal investigations and prosecutions of trademark violations.

- In March 2019, at the National Advocacy Center in Columbia, South Carolina, CCIPS hosted its annual conference and training for the Computer Hacking and Intellectual Property prosecutors (CHIPs) in each of the 93 U.S. Attorneys Offices and Main Justice Components. The conference provided CHIP prosecutors with the latest guidance on issues of electronic evidence gathering, digital forensics, computer crime, intellectual property crime, and related issues. More than 150 CHIPs attended the four day conference.

- In April 2019, CCIPS presented at an Intellectual Property and Trade Enforcement Investigations (IPTEI) course at the IPR Center in Arlington, Virginia, to approximately 30 HSI and CBP agents. The presentation covered relevant law and policy, provided 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 April 2019, CCIPS presented its Intellectual Property Crimes Seminar at the National Advocacy Center to an audience of 80 prosecutors and federal agents. The Seminar provided

in-depth instruction on investigating and prosecuting trafficking of counterfeit goods and services, criminal copyright infringement, and theft of trade secrets, along with electronic evidence gathering for IP cases. The IP Seminar was organized by CCIPS.

- In May 2019, CCIPS Attorneys addressed approximately 20 participants at the DOJ/OPDAT Resident Legal Advisor ("RLA") School in Washington, DC. CCIPS' and DOJ's work on cybercrime, intellectual property, and electronic evidence issues in the United States and around the world were discussed.

- In June 2019, CCIPS presented at an Intellectual Property and Trade Enforcement Investigations (IPTEI) course at the IPR Center in Arlington, Virginia, to approximately 30 HSI and CBP agents. The presentation covered relevant law and policy, provide practical guidance in counterfeit trademark investigations, and include 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 July 2019, at the U.S. Patent and Trademark Office in Alexandria, Virginia, CCIPS gave a presentation about dealing with trade secrets and economic espionage issues overseas at the annual State Department Foreign Service Institute intellectual property rights training course for Foreign Service officers and other State Department employees. The course included about a dozen officers assigned to posts in Egypt, Colombia, Romania, Azerbaijan, Suriname, and the U.S.

- On August 2019, CCIPS and an AUSA presented on the "Prosecutor's Perspective" of intellectual property investigations and prosecutions to special agents with the Federal Bureau of Investigation. The presentation was part of the FBI's Intellectual Property Rights Operations Public-Private Coordination Meeting in Chicago, Illinois.

- In August 2019, CCIPS presented at an Intellectual Property and Trade Enforcement Investigations (IPTEI) course at the IPR Center in Arlington, Virginia, to approximately 30 HSI and CBP agents. The presentation covered relevant law and policy, provide practical guidance in counterfeit trademark investigations, and include case studies of *U.S. v. Peter Picone* and *U.S. v. Rogelio Vasquez*, who were convicted of selling counterfeit integrated circuits to the military.

- During FY 2019, CCIPS addressed participants at multiple sessions of the DOJ/OPDAT Resident Legal Advisor ("RLA") School in Washington, D.C. CCIPS spoke regarding CCIPS' and DOJ's work on cybercrime, intellectual property, and electronic evidence issues in the U.S. and around the world as well as the ICHIP Network.

International Outreach and Training

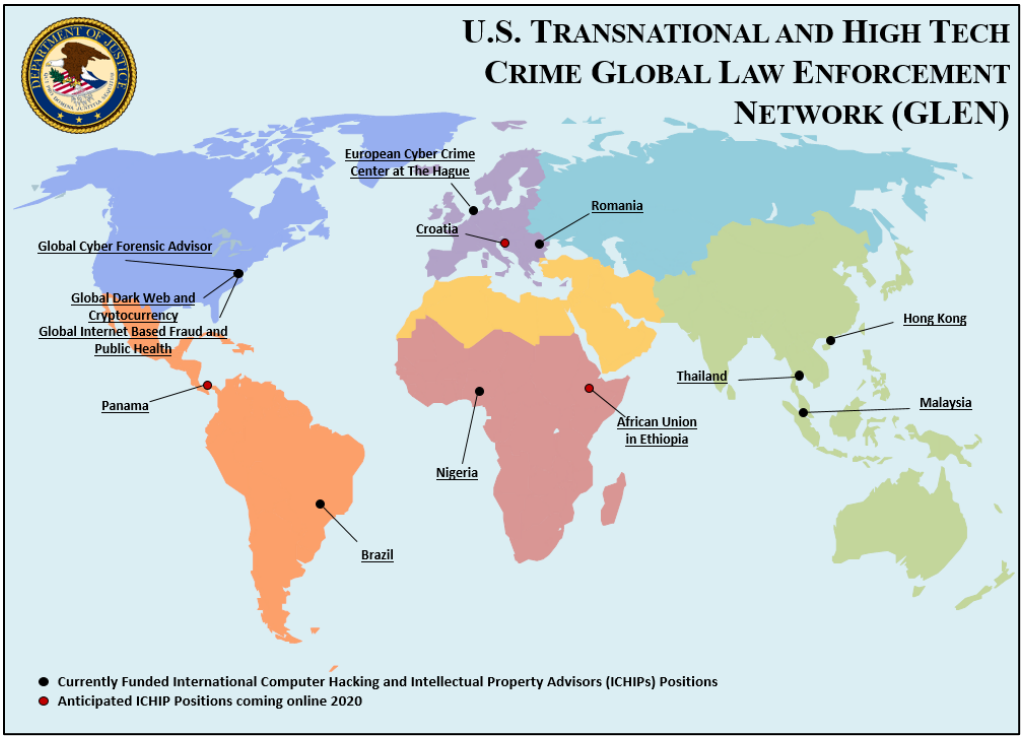
Global IP crime, from the manufacture and worldwide distribution of counterfeit goods, to the sprawling online businesses designed to reap profits from the distribution of copyrighted works, continues to grow and change in an effort to stay ahead of law enforcement. As a world

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 2019, 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 2019 to provide training to foreign officials on effective enforcement of IP laws. The Department'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 2019, the Department, with assistance from the State Department, continued to expand the U.S. Transnational and High Tech Crime Global Law Enforcement Network ("GLEN") of International Computer Hacking and Intellectual Property ("ICHIP") attorneys (formerly, the Intellectual Property Law Enforcement Coordinator ("IPLEC") program). DOJ has now posted experienced prosecutors in Bucharest, Romania; Hong Kong; Sao Paolo, Brazil; Abuja, Nigeria; Bangkok, Thailand; Kuala Lumpur, Malaysia; and The Hague, Netherlands. The GLEN also now includes two ICHIPs based in Washington, D.C. to assist the regional ICHIPs with the subject matter areas of Global Dark Web and Cryptocurrency issues and Global Internet Based Fraud and Public Health issues. The GLEN also now includes a Global Cyber Forensic Advisor also based in Washington, D.C. In 2020, the GLEN will expand to include regional ICHIPs based in Panama City, Panama; Zagreb, Croatia; and Addis Ababa, Ethiopia.[7]

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



Examples of DOJ's international engagement regarding criminal IP enforcement include:

ASIA

Intellectual Property Training in Vietnam. In October 2018, CCIPS, along with the Hong Kong ICHIP; U.S. District Court Judge Berg; and DHS, participated in judicial exchange and training workshops in Hanoi and Ho Chi Minh City, Vietnam, focusing on criminal enforcement of intellectual property laws. Vietnam's national legislature enacted significant amendments to strengthen the country's criminal intellectual property laws. The program, organized by the Hong Kong ICHIP, is designed to assist Vietnam's Supreme People's Court in developing guidance for lower courts to implement these new changes to Vietnam's criminal laws, and to share best practices on IP enforcement with Vietnamese prosecutors, judges, and other officials.

Workshop for the Association of Southeast Asian Nations ("ASEAN") Members on Cyber-Enabled IPR. In October 2018, the Hong Kong ICHIP, in collaboration with the Kuala Lumpur ICHIP, presented a workshop in Singapore on cyber-enabled IPR crime for 32 police, prosecutors and IPR administrative officials from the ASEAN member states and Timor-Leste. The Singapore IP Academy, the Singapore IP Office, collaborated on the workshop under the auspices of the Third Country Training Programme, a joint initiative of Singapore and the U.S. to conduct capacity-building activities in Southeast Asia. CCIPS and HSI representatives also served as instructors at the workshop.

Follow-Up Meeting with Kazakhstan Minister of Justice. In November 2018, CCIPS and other U.S. government representatives met at the IPR Center in Arlington, Virginia with the Kazakhstan Minister of Justice to discuss intellectual property issues. This meeting followed up a

previous discussion CCIPS had with the Minister last April on software piracy issues as well as other conversations with Ministry of Justice staff last spring and summer.

Presentation at USPTO's Pakistan Intellectual Property Judicial Exchange. In December 2018, CCIPS presented at the U.S. Patent and Trademark Office's Pakistan Intellectual Property Judicial Exchange. The audience consisted of 14 judges and attorneys who will be assigned to IP Tribunals in Pakistan. The five-day program, held at the Global Intellectual Property Academy in Alexandria, Virginia, is designed to provide a comprehensive overview of U.S. intellectual property law. CCIPS presented background, case studies and sentencing issues related to criminal copyright, trademark and trade secret investigations and prosecutions.

Colloquium on Civil and Criminal IP Infringement. In January and February 2019, the Bangkok ICHIP and the Hong Kong ICHIP participated as instructors at a "Judicial Colloquium on Civil and Criminal Infringement of Intellectual Property," for approximately 30 judges handling IPR cases from the Association of Southeast Nations (ASEAN) member states in Bangkok, Thailand. The USPTO Global Intellectual Property Academy (GIPA) and the ASEAN Secretariat co-sponsored the program. Three U.S. federal judges also participated as instructors. The ICHIPs led a discussion of the primary recurring issues in IP criminal prosecutions, such as proving a defendant's mental state, valuing IP-infringing goods and content, and protecting trade secrets during litigation.

Meetings with Chinese Officials on IPR Enforcement. In March 2019, the Hong Kong ICHIP traveled to Shanghai and Beijing, China for a series of meetings with government officials focused on IPR enforcement and private stakeholders. In Shanghai, the ICHIP attended an IPR forum organized by the Beijing-based DHH (Shanghai) law firm, and presented on criminal enforcement of trade secrets protection. In Beijing, the ICHIP and OPDAT China RLA met with prosecutors from the Haidian District Procuratorate, including the chief prosecutors from both its IPR and cybercrime sections. Also in Beijing, the ICHIP, RLA, and USPTO Beijing IP Attaché met with three prosecutors from the Supreme People's Procuratorate.

Asia Regional Workshop Against Trade in Counterfeit Food, Beverages, Cosmetics and Fast Moving Consumer Goods. In April 2019, the Hong Kong ICHIP staged the "Asia Regional Workshop on Enforcement Against Trade in Counterfeit Food, Beverages, Cosmetics and Fast Moving Consumer Goods," with primary co-sponsors USPTO and the Vietnam Ministry of Science and Technology, in Ho Chi Minh City, Vietnam. The workshop brought together approximately 75 police officers, prosecutors, customs officials and IPR policy-makers from Bhutan, Cambodia, China, the Commonwealth of the Northern Mariana Islands, Fiji, India, Indonesia, Laos, Malaysia, Mongolia, Myanmar, Nepal, Pakistan, Papua New Guinea, the Philippines, Qatar, Saudi Arabia, Sri Lanka, Thailand, Timor-Leste, Vanautu and Vietnam – and over 50 presenters from Vietnam and the rest of Asia, the U.S., and Europe. The workshop included sessions on statutory approaches to IPR enforcement, tackling online trafficking of counterfeit goods, gathering intelligence and conducting IPR investigations, transnational cooperation to fight IPR crime, and several case studies from law enforcement and industry of international investigations and prosecutions involving counterfeit ingestibles and topicals. CCIPS participated in a number of panels, including ones tailored to combatting organized crime in counterfeiting, facilitating cooperation in the tackling of largescale counterfeit actors, and

implementing deterrence-based strategies. The workshop culminated in a discussion of a whole-of-government approach to combatting counterfeit goods. In addition to participation from the Department of Justice and USPTO, representatives from the State Department, FBI, FDA, CBP, and DHS also contributed to the workshop.

Participation in International IP-Protection Workshops in Taiwan. In April 2019, Hong Kong ICHIP and CCIPS joined representatives from the U.S. judiciary, USPTO, DHS, and FBI in two day-long IP workshops in Taipei, Taiwan: Best Practices for Stemming Digital Piracy and Best Practices for Enforcement of Trade Secret Protection. The U.S. delegates joined representatives from the Taiwan Ministry of Justice, the American Institute in Taiwan, and members of the Taiwan Intellectual Property Court to discuss international best practices for protecting intellectual property. In advance of the workshops, the U.S. delegates spent three days meeting with various Taiwanese law enforcement and industry stakeholders to discuss pressing issues related to digital piracy and trade secret theft.

Cyber and IP Meeting with Kazakhstan Officials. In May 2019, CCIPS met in Washington, D.C., with six officials from Kazakhstan regarding combating cyber and intellectual property offenses. The officials came from the Prosecutor General's Office, Ministry of Internal Affairs, Ministry of Defense, and Committee for National Security. Topics included cybercrime, cybersecurity, software piracy, and international cooperation.

Meeting with Law Enforcement Representatives from Taiwan. In May 2019, CCIPS and the Office of International Affairs ("OIA") met at OIA's offices with representatives of Taiwan's law enforcement based in Washington to discuss common challenges faced in investigating and prosecuting intellectual property cases, and potential cooperation regarding investigation of online piracy.

Meeting with Delegation from Myanmar Regarding Electronic Evidence and IP Issues. In May 2019, CCIPS met with ten prosecutors from Myanmar to discuss cyber and intellectual property crimes, with a focus on how to investigate and prosecute cybercrime and best practices for organizing, storing, and sharing electronic evidence in court.

Regional Judicial Training Conference for Judges from Kazakhstan, the Kyrgyz Republic, Tajikistan, and Turkmenistan. In May 2019, CCIPS participated in a three-day training conference in Nur-Sultan, Kazakhstan for judges from four countries in Central Asia: Kazakhstan, the Kyrgyz Republic, Tajikistan, and Turkmenistan focusing on protection of IPR. USPTO organized the conference for approximately 20 judges in conjunction with the U.S. Embassy in Nur-Sultan and DOJ. CCIPS gave five presentations on various issues; led a discussion of a case study; played the prosecutor in a mock sentencing hearing; and also participated in additional panels and discussions. Other presenters included U.S. federal judges, and the U.S. Ambassador to Kazakhstan and Vice Minister of Justice of Kazakhstan also spoke at the conference.

Participation in Bangladeshi IP Roundtable. In May 2019, the Hong Kong ICHIP participated in a roundtable on IP issues and concerns in Dhaka, Bangladesh, organized by the USPTO Office of South Asia, and headlined by visiting U.S. Assistant Secretary of Commerce and Director

General of the U.S. Foreign Commercial Service Ian Steff. The ICHIP offered suggestions on strengthen criminal enforcement of IP rights in Bangladesh.

Regional Workshop for ASEAN Member States. In June 2019, the Hong Kong ICHIP traveled to Bangkok, Thailand, where, along with the Bangkok Asia ICHIP and USPTO, he staged a regional workshop on IPR enforcement for prosecutors, attended by seven ASEAN member states. The Hong Kong Asia ICHIP moderated panels on IPR investigative methods, the nexus between IPR and organized crime, and statutory approaches to IPR enforcement. The Hong Kong ICHIP also created an interactive electronic evidence scenario which the participants used for mock evidentiary hearings.

Cyber/Digital Evidence Program for Thai Judges. In June 2019, the Kuala Lumpur ICHIP assisted with the organization and implementation of a Cyber/Digital Evidence program for 35 members of the Thai Judiciary co-organized with and hosted by the University of California, Berkeley, School of Law. The program was designed to strengthen the participant's knowledge of cybercrime, intellectual property, digital evidence, and cybersecurity through lectures, site visits, and group discussions with U.S. judges.

Presentation to Visiting Chinese Delegation on IPR: In July 2019, CCIPS addressed a visiting group of Chinese government officials as well as private sector 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.

Presentation to Mongolian Delegation on Criminal IP Issues. In September 2019, CCIPS addressed a Mongolian delegation from the Judicial General Council of Mongolia. CCIPS presented on DOJ's role in IP enforcement and on investigating and prosecuting IP crimes in the United States, and the group discussed the potential for future training opportunities.

NORTH AFRICA AND THE MIDDLE EAST

Meeting with United Arab Emirates Delegation on Intellectual Property and Other Issues. In March 2019, CCIPS met with a delegation from the United Arab Emirates ("UAE") headed by a Major General from the Dubai Police. The group included the leaders of the Emirates Intellectual Property Association; director of the UAE Trademarks Department; head of the UAE Brand Owners' Protection Group; head of Louis Vuitton Middle East; and an official from the UAE Embassy to the U.S. Discussion topics included UAE's implementation of the 2016 Combating Commercial Fraud law (which provides new powers to UAE authorities to seize and destroy illicit goods even within FTZs), customs best practices, internet piracy, sentencing in IPR cases, cybercrime and cybersecurity, and international law enforcement cooperation.

CENTRAL AND SOUTH AMERICA

Participation in International Anti-Counterfeiting Coalition Latin America Summit. In October 2018, the Brazil ICHIP participated in the second International Anti-Counterfeiting Coalition ("IACC") Latin America regional brand protection summit in Orlando, Florida. The Brazil ICHIP discussed trending issues in online and hard goods IPR enforcement as well as cross-

border collaboration on cases and investigations with police, prosecutors, rights-holders, and customs agents from Argentina, Brazil, Uruguay, Paraguay, Honduras, Guatemala, El Salvador, Barbados, Trinidad, Suriname, Peru, and Costa Rica.

Presentation on Criminal Copyright Issues in Caribbean. In December 2019, the Brazil ICHIP Foreign Service National ("FSN") presented on criminal copyright infringement statutes and trends in digital piracy at the Caribbean College of Justice's annual conference in Kingston, Jamaica. The FSN addressed approximately 100 participants, mainly judicial officers, regarding the elements of criminal copyright statutes in the United States and trends in digital piracy, such as the growth of pirated Internet Protocol television (IPTV) devices, camcording, and websites that support illicit streaming.

"Going Dark" Conference in Brazil. In February 2019, the Brazil ICHIP and other DOJ colleagues attended the first-ever Going Dark conference in Brasilia. The conference focused on addressing emerging challenges to law enforcement posed by the growing use of encryption technologies to hinder the investigation and prosecution of a variety of crimes, particularly complex cyberattacks, terrorism, drug trafficking, online trademark and copyright infringement, and other transnational organized crime activity. Approximately 40 participants from Brazilian local and federal law enforcement agencies attended the program as well as enforcement officials from other countries, including Australia, Belgium, France, Colombia, India, and Poland.

Training for Central American Judges. In March 2019, On March 4-6, the Brazil ICHIP trained approximately 40 judges drawn from around Central America in Tegucigalpa, Honduras, at a USPTO-sponsored regional enforcement program on best practices in presiding over civil and criminal IP litigation. The ICHIP covered the elements and penalties for trademark and copyright infringement in the U.S. and how police and prosecutors investigated these crimes and gathered powerful electronic evidence in these cases to present to judges and juries. The ICHIP also explained the criteria prosecutors use to arrive at deterrent but fair sentences in these cases and also highlighted the value of additional charges like conspiracy and money laundering in these cases.

IP Training Conference for Argentinian Law Enforcement Officials. In April 2019, CCIPS participated in a three-day USPTO-sponsored training conference in Buenos Aires, Argentina, for approximately 65 Argentinian judges, prosecutors, police, gendarmerie, customs officers, airport police, coast guard officers, intelligence analysts, and other officials focusing on protection of intellectual property rights. Other speakers included the U.S. ambassador to Argentina, the national director of investigations at the Argentinian Ministry of Security, the national director of international cooperation at the Ministry of Security, and experts from the USPTO, DHS, FBI, Virginia State Police, and the Argentinian private sector.

Participation in USPTO Regional IPR Workshop in Panama. In April 2019, CCIPS participated at a USPTO-sponsored IPR seminar in Panama City, Panama. The seminar was co-sponsored by various Panamanian ministries and the World Customs Organization. In two sessions, CCIPS spoke on criminal enforcement of intellectual property rights in the United States and on the use of electronic evidence for valuation in IP cases.

Regional Training Program on Digital Piracy. In May 2019, the Brazil ICHIP, CCIPS, and the USPTO trained approximately 50 prosecutors and police from Colombia, Chile, and Peru, at a regional program on digital piracy in Bogota, Colombia. The Motion Picture Association of America and the Recording Industry Association of America led industry presentations during the program. Presenters described different internet platforms used to facilitate digital piracy, including peer-to-peer networks and pirate apps and services available for download to Internet Protocol Television set top boxes (IPTV). Participants learned how to use different open source tools to investigate pirate websites as well as to preserve and analyze electronic evidence from digital devices. Foreign counterparts also provided case studies detailing their successes and challenges in investigating and prosecuting cases of digital IPR crime.

Latin American Workshop on Cyber-Enabled IPR Crime. In May 2019, CCIPS participated in a Digital Piracy Workshop on Challenges and Best Practices for Prosecutors and Police in Bogota, Colombia. The workshop was organized by the Brazil ICHIP and the USPTO. The workshop trained police and prosecutors from various Latin American countries on a variety of topics, including general IP enforcement, methods for valuation, IP crimes committed through online forums, investigative techniques, undercover operations, and digital forensics. Various rights holders and regional stakeholders also addressed how to more effectively work with industry to protect IP rights.

Electronic Evidence Training for Cyber-Enabled IP Crime. In June 2019, at a program in Santiago, Chile, the Brazil ICHIP and CCIPS trained approximately 60 Chilean police and prosecutors on the handling of electronic evidence in cybercrime investigations, including cyber-enabled IP crime. Representatives from Facebook/Instagram and Uber participated in a panel for providers to share their insights on collaboration with law enforcement, especially on requests for overseas data. The program included a practical tabletop exercise on locating a target of a crime using open source applications, third-party data, and traditional methods of investigation.

Meeting with Delegation from Latin America on IP, Trade, and Investment Issues. In June 2019, CCIPS met in Washington, D.C., with 11 government officials and private sector representatives from Bolivia, Colombia, Ecuador, Guatemala, Honduras, Mexico, and Uruguay regarding intellectual property, trade, and investment issues in the United States and Latin America. The delegation learned about the U.S. perspective on a number of trade issues as part of the State Department's International Visitor Leadership Program.

EUROPE

Meetings with Delegation from Austrian Ministry of Justice. In November 2018, CCIPS spoke with a delegation from the Austrian Minister of Justice as one of several presenters discussing the role of the Criminal Division and specific components. CCIPS discussed how CCIPS functions in conjunction with the USAOs, other DOJ sections, and international counterparts to combat cyber and intellectual property crime. The meetings was hosted by Deputy Assistant Attorney General Bruce Swartz and also included presentations from the Money Laundering and Asset Recovery Section and Fraud Section.

Container Security Workshop for European Countries. In November 2018, the Romania ICHIP, in partnership with Southeast European Law Enforcement Center, organized a container security workshop for law enforcement from Albania, Bosnia and Herzegovina, Bulgaria, Greece, Hungary, Macedonia, Moldova, Montenegro, Romania, Serbia, Turkey, Cyprus, Georgia and Ukraine. The first day of the program consisted of classroom activities with interactive presentations focused on container training, identification and interdiction of counterfeit goods, new technology used to track containers around the world, investigation and prosecution of IPR cases. In addition to the ICHIP, the instructors included personnel from HSI, CBP, Michigan State University, and industry representatives. On the second day, representatives from Romanian Customs and Romanian Police representatives delivered presentations, and attendees visited the Romanian Border Police Headquarters where the General Inspector of the Romanian Border Police spoke to the group. Following the presentation, attendees viewed a live demonstration at their center for border surveillance of the System for Surveillance and Control of the Maritime Traffic on the Black Sea (SCOMAR) and several databases and tools used in their daily activities.

IP Criminal Enforcement Training for Romanian Police Academy. In March 2019, the Romania ICHIP organized a two-day "Introduction to IP Criminal Enforcement" training for students at the Romanian Police Academy. The audience consisted of 600 future police officers who will be deployed across Romania after graduating from the Academy. The program was designed to increase awareness and enthusiasm for identifying and investigating intellectual property crimes, and included case studies by the Romania ICHIP as well as a Romanian prosecutor-investigator team specializing in complex internet piracy cases. In addition, EUIPO and USPTO presenters addressed the importance of intellectual property rights and the policy reasons behind robust intellectual property enforcement.

Europol Anti-Piracy Seminar in The Hague. In March 2019, the Romania ICHIP presented at the Anti-Piracy Seminar organized by Europol and the International Federation of the Phonographic Industry in The Hague, Netherlands. The seminar covered all aspects of modern piracy prevention and enforcement, including new technologies in the arenas of torrent sites, cyber lockers, linking or referral sites, and stream ripping. The Romania ICHIP addressed cooperation between law enforcement and industry as well as open source investigative methods available to resource-strapped law enforcement actors.

Regional Workshops on Cyber-Enabled IP Crime. In May 2019, the Romania ICHIP team organized back-to-back workshops in Romania and Hungary. The workshops, entitled "New Developments in Computer-Facilitated Intellectual Property Crimes" convened law enforcement and judiciary representatives from across the two countries. The program addressed IP crime trends, cryptocurrency issues, financial investigations, international legal assistance and cooperation, and electronic evidence issues. The Romania ICHIP team and USPTO Brussels had a follow-up meeting with the Romanian Vice Prime Minister on the development of a National IP Strategy. The Romania ICHIP team also organized in partnership with the Romanian Football Federation (FRF), a half-day conference "Reach for Gold: IP and Sports" at the FRF Headquarters to celebrate World Intellectual Property Day. High-level Romanian officials participated in the program, which highlighted the positive role that IP enforcement plays with

respect to the sports industry and also addressed the continued challenge of making IP enforcement a priority in Romania.

SUB-SAHARAN AFRICA

IP Meeting with Nigerian Officials. In October 2018, CCIPS met with a seven-person delegation from Nigeria (including officials from their food & drug agency, consumer protection council, trademark office, and a prosecutor) in Washington, D.C. to discuss U.S. criminal enforcement of Intellectual Property rights. OPDAT facilitated the meeting, which was a part of the U.S. State Department's International Visitor Leadership Program.

Meeting with IPR Stakeholders. In October 2018, the Nigeria ICHIP traveled to Kenya and Botswana for numerous meetings. In Kenya, the ICHIP met with several IPR stakeholders, including representatives from the Kenya Copyright Board; Anti-Counterfeit Agency, a dynamic interagency IP enforcement group in Kenya; Kenya Pharmacy and Poisons Board; INTERPOL; Office of the Attorney General and Department of Justice; and Office of the Director of Public Prosecutions. In Botswana, the ICHIP met with representatives from the Botswana Medicines Regulatory Authority; Narcotics Bureau of the Botswana Police; Botswana Companies and Intellectual Property Authority; Department of Public Prosecutions; Customs Department; and local and international pharmaceutical companies as well as U.S. Embassy officials and International Law Enforcement Academy ("ILEA") staff.

Eastern and Southern Africa Workshop on Pharmaceutical Crimes. In November 2018, the Nigeria ICHIP organized the Eastern and Southern Africa Workshop to Build Enforcement Capacity and Improve Regional Coordination in Combatting Pharmaceutical Crimes, held at the ILEA in Gaborone, Botswana. Representatives from Botswana, Zambia, Namibia, Kenya, Tanzania, Malawi, Rwanda, and Uganda attended the program, and participants included police, prosecutors, health regulatory officials, gendarmerie, investigative magistrates, and customs officials. In addition to the ICHIP team, workshop instructors included personnel from HSI, the Southern District of Florida, a prosecutor's office in Kenya, INTERPOL, and the pharmaceutical industry.

USPTO IPR Program for Sub-Saharan Africa. In April 2019, the Nigeria ICHIP, together with two U.S. Federal Judges; USPTO; the Africa Regional Intellectual Property Organization (ARIPO); and Embassy Gaborone, organized and led a USPTO-sponsored Intellectual Property Rights (IPR) capacity-building program for judges and lawyers from 13 sub-Saharan Africa nations. This workshop sparked judges' eagerness to acquire more IPR education and prompted from them numerous ideas and suggestions for next steps. The ICHIP, USPTO, and ARIPO will assist the development of a regional IPR judicial resource/toolkit/manual for sub-Saharan Africa, create a repository for decided IPR cases in sub-Saharan Africa to be lodged with ARIPO, and aid in developing a formal IPR network of judges. This collaborative workshop served to raise IPR awareness, begin a definitive process for enhancing IPR capacity among sub-Saharan African judges, and start the process of developing a cohort of African judges competent in IPR enforcement.

World Intellectual Property Day Event. In May 2019, the Nigeria ICHIP worked with the Embassy's Public Affairs Section to highlight the importance of IP enforcement in Nigeria and the United States. The Rosa Parks American Center, in collaboration with the Economic Section, hosted approximately 70 young Nigerian entrepreneurs in honor of World Intellectual Property Rights Day. The program commenced with a film screening entitled "The First 20 Million Is Easy." After the movie, a Nigerian entrepreneur led a discussion on how intellectual property impacts entrepreneurs. The Nigeria ICHIP advised the group of pending legislation in Nigeria to strengthen IP enforcement and, as part of the discussion, also highlighted the importance of IP to the United States.

Regional IP Workshop for Prosecutors and Law Enforcement. In May 2019, the Nigeria ICHIP organized the "Regional Train-the-Trainers Intellectual Property Enforcement Workshop for Police Instructors and Prosecutors" at the ILEA in Gaborone, Botswana. The ICHIP coordinated with the World Intellectual Property Organization (WIPO), the African Regional Intellectual Property Organization (ARIPO), and CCIPS in conducting the program. Law enforcement and prosecution representatives from Lesotho, Sierra Leone, Liberia, Malawi, the Gambia, Zambia, Mozambique, Botswana, and Nigeria attended and participated actively in the program.

Presentation at Botswana-based International Law Enforcement Academy. In May 2019, the Africa ICHIP organized the "Regional Train-the-Trainers Intellectual Property Enforcement Workshop for Police Instructors and Prosecutors" at the ILEA in Gaborone, Botswana, in coordination with the World Intellectual Property Organization (WIPO) and the African Regional Intellectual Property Organization (ARIPO). CCIPS participated in the program, and presented on the following topics: overview of the United States' approach to IP enforcement; elements of trademark counterfeiting and copyright/internet piracy; charging considerations and prosecutorial decisions; introduction to computer crimes and digital evidence; and collection and preservation of digital evidence.

ICHIP Conference on Counterfeit Pharmaceuticals and Pesticides. In June 2019, the Africa ICHIP organized the "Workshop to Build Enforcement Capacity and Improve Coordination in Combatting Pharmaceutical Crimes & Illicit Pesticides." The program took place in Dakar, Senegal and included law enforcement officials from francophone nations including Senegal, the Republic of Congo, Chad, Burundi, Guinea, Côte D'Ivoire, Democratic Republic of the Congo, Gabon, Mali, Mauritania, and Morocco. Presenters, including a CCIPS attorney, discussed regional legal challenges to enforcement, identification of counterfeit products, and models to better combat the trade in counterfeit and illicit pharmaceuticals and pesticides.

Presentation at Intellectual Property Symposium. In September 2019, the Africa ICHIP organized the "Intellectual Property Symposium: The Bane of Counterfeit Pharmaceuticals and Piracy," hosted in Lagos, Nigeria, which was sponsored by the Nigerian National Agency for Food and Drug Administration and Control (NAFDAC) in coordination with the United States Embassy – Nigeria and the Africa ICHIP. The symposium's theme was building respect for intellectual property rights as a strategic resource for economic growth, and the symposium focused on the threats of fake drugs on the continent of Africa and the financial impact of copyright piracy on both the national economy and innovators. CCIPS participated in the event, and presented on U.S. counterfeit medicine case scenarios and facilitated a panel discussion on

best practices for investigating and prosecuting counterfeit drug cases as well as collaborating with both industry and law enforcement partners.

Presentation at African Regional Workshop. In September 2019, the Africa ICHIP organized the "African Regional Workshop on Cybercrime, National Cyber Security, and Internet Piracy," hosted in Lagos, Nigeria, and sponsored by U.S. Department of State's Bureau of International Narcotics and Law Enforcement.. The workshop addressed building an understanding of online crimes and electronic evidence, the development of national cyber security policy and strategies, internet piracy investigations, and the Budapest Convention. CCIPS participated in the workshop, and presented on internet piracy criminal enforcement, digital evidence in piracy prosecutions, cybercrime, and cyber self-defense.

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 FY 2019, CCIPS organized and planned its Twelfth Annual IP Industry and Law Enforcement Meeting held in Washington, D.C, in October 2018. The yearly meeting provides representatives from a broad range of industries with an opportunity to communicate directly with the law enforcement agents and prosecutors most responsible for federal criminal enforcement of IP law at the national level. This year, Assistant Attorney General Brian Benczkowski provided keynote remarks, and several senior DOJ and law enforcement officials participated in the meeting. Approximately 100 government and 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, as well as the Civil Division's Consumer Protection Branch 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 2018, CCIPS presented at Michigan State University's Center for Anti-Counterfeiting and Product Protection (A-CAPP) Brand Protection Strategy Summit on a panel entitled "What Everyone Ought to Know about the Relationship of Counterfeiting with Other Crimes." The panelists discussed the overlap between intellectual property crimes and other crimes such as fraud, forced labor, and human trafficking, in addition to the role that intellectual property crimes play in financing transnational organized crime and terrorist networks. National IPR Center, Western Union, and Michigan State University representatives also served on the panel.

- In October 2018, CCIPS and the District of Connecticut U.S. Attorney's Office provided a trade secret theft and economic espionage briefing for Raytheon Company in Waltham, Connecticut. The attendees included Raytheon's in-house counsel, outside counsel, IT specialists, and engineers. The briefing addressed various topics including the elements of the criminal trade secret theft and economic espionage statutes, how to

satisfy the statutes' reasonable measures prong, best practices for protection of trade secrets when collaborating with other military contractors, and data rights ownership when military contractors are working with the government. Defense Criminal Investigative Service and the District of Massachusetts' CHIP AUSA participated in the program as well.

- In October 2018, CCIPS took part in a panel discussion in New York City addressing the U.S. government's role in copyright enforcement. CCIPS joined representatives of DOJ's Civil Division and the U.S. Copyright Office to address an audience of approximately 400 representatives of the entertainment and copyright content industries. CCIPS addressed the role of CCIPS and the CHIP Network and the process of investigating and prosecuting criminal copyright cases.

- In November 2018, CCIPS and the IPR Center co-hosted a half-day meeting of the Counterfeit Microelectronics Working Group to discuss ways to detect and prevent distribution of counterfeit microelectronics in the U.S. supply chain. The meeting included speakers from CBP – Office of Trade, Underwriters Laboratories, the Air Force Office of Special Investigations, and a presentation from a CCIPS Attorney. Approximately 60 industry, government, and law enforcement representatives attended.

- In November 2018, CCIPS presented at the Annual Meeting of the IP Law Section of the California Lawyers Association, known as the 43rd Annual Intellectual Property Institute in San Jose, California. CCIPS addressed *United States v. Sinovel* and working with Department of Justice to fight cybercrime and intellectual property crime. More than 200 intellectual property attorneys were in attendance.

- In December 2018, CCIPS spoke at an event hosted by the International Trademark Association and Global Intellectual Property Center, entitled "What You Need to Know about Counterfeit Products During the Holiday Shopping Season: A Congressional Briefing and Conversation over Lunch." CCIPS' presentation focused on how CCIPS works with prosecutors, agents, rights holders, and other stakeholders to deter trafficking in counterfeit goods and services. Approximately 70 members of the public attended the briefing.

- In March 2019, CCIPS participated in a panel discussion in Washington, D.C., at the Federal Circuit Bar Association's event entitled "Key Issues Shaping the U.S. IP Landscape." The panel focused on U.S. government agencies' views regarding IP as a driver for innovation, and CCIPS specifically addressed DOJ's efforts and priorities with respect to IP criminal enforcement. Other panelists included USPTO and Federal Trade Commission (FTC) representatives.

- In April 2019, CCIPS presented at a round table discussion at the University of California Berkeley Law School entitled "Tech, Trade and China: A Progress Report One Year Into the Trade War." CCIPS discussed the Department's China Initiative, and efforts to address trade secret theft and trafficking in counterfeit goods through criminal enforcement and international engagement. Presenters included representatives of U.S.

agencies, U.S. and Chinese legal practitioners, and experts in technology and international trade.

- In April 2019, CCIPS participated in a working group convened as part of Operation Body Armor at the National IPR Coordination Center in Crystal City, Virginia. The working group included representatives from several major companies in the personal care products industry and federal law enforcement agents from around the country. This day-long meeting sought to foster communication between industry and law enforcement and encourage cooperation within and among the industries. CCIPS gave the working group an overview of DOJ's role in this and similar efforts, including an explanation of CCIPS' interaction with U.S. Attorney's Offices around the country and law enforcement around the world, the primary criminal IP offenses CCIPS prosecutes, and the criminal referral process as well as resources for victims of IP crimes.

- In May 2019, CCIPS presented at an annual meeting of the Michigan IP Law Association. The presentation provided an overview of the latest cyber and IP threats. The presentation also covered the importance of attorneys developing relationships with law enforcement in advance of a cyber incident or IP theft, as well as the importance of alerting law enforcement as soon as possible after an incident does occur. In addition, the presentation addressed common concerns and misconceptions associated with involving law enforcement in these matters.

- In May 2019, CCIPS and the IPR Center co-hosted a one-day meeting of the Counterfeit Microelectronics Working Group at the IPR Center, to discuss ways to detect and prevent distribution of counterfeit microelectronics in the U.S. supply chain. CCIPS, in conjunction with the IPR Center and industry partners, organized the meeting. The IPEC provided keynote remarks, and the meeting included speakers from Customs and Border Protection – Office of Trade, the U.S. Postal Service, the Cybersecurity and Infrastructure Agency, as well as presentations from NSD CES. Approximately 75 industry, government, and law enforcement representatives attended.

- In July 2019, CCIPS presented at the Symposium on Counterfeit Parts and Materials in College Park, Maryland. The Symposium, organized by the Surface Mount Technology Association (SMTA) and the Center for Advanced Life Cycle Engineering (CALCE), included an audience of over 90 representatives in academia, manufacturing, technology, law, government and military. CCIPS presented a case study of *United States v. Rogelio Vasquez* and discussed the challenges faced in federal prosecutions involving counterfeit integrated circuits.

- In July 2019, CCIPS participated on a panel entitled "Where Did All the Files Go?: Investigating, Prosecuting, Defending Data Theft Cases." An NSD CES attorney and two private sector employees served as co-panelists. The panel addressed U.S. laws currently in place to protect trade secret information, trade secret and economic espionage enforcement priorities and trends, and best practices for reporting trade secret theft to U.S. law enforcement.

- In August 2019, CCIPS presented at an international security conference hosted by ASIS International in Sunnyvale, California. CCIPS' presentation focused on working with the Department of Justice to prevent, respond to, and deter theft of trade secrets and cybercrime. More than 250 business leaders and cybersecurity professionals attended the conference.

- In September 2019, CCIPS presented at the 24th Annual Fraud and Anti-Counterfeiting Conference in Toronto, Canada. CCIPS participated on a panel discussing and promoting cooperation between government and industry, and addressed the role of CCIPS, the ICHIP attorneys and the CHIP Network in combatting counterfeit goods. The conference included approximately 150 attendees from industry, law enforcement and other government personnel.

- In September 2019, CCIPS presented at the USPTO symposium "Trending Issues in Trade Secrets: 2019." CCIPS, NSD CES, and FBI addressed selected issues in criminal trade secret prosecutions. CCIPS and the District of Kansas discussed notable trade secret theft cases they have prosecuted. Approximately 80 in-person attendees and approximately 300 remote attendees, consisting primarily of law firm and in-house practitioners and subject-matter experts, participated in the symposium.

- In September 2019, CCIPS presented on a panel discussion alongside FBI and HSI representatives entitled "Counterfeits and the Dark Web Distribution and Supply Chain," at Michigan State University's (MSU's) Brand Protection Strategy Summit. The panelists provided an overview of the role of dark web markets as a means to buy and sell counterfeit products among other illicit goods and services. CCIPS also participated in a "Spark Table," which was designed to showcase the U.S. federal, state and local government resources available relevant to brand protection professionals' efforts to combat counterfeiting.

- In September 2019, CCIPS spoke at the 23rd Annual Conference of the Bar Association of the Eastern District of Texas. CCIPS participated on two panels – one addressing the relevant factors when considering federal prosecution for trademark infringement, and another on best practices for defining and protecting trade secrets in civil and criminal litigation. The conference included over 500 attendees from industry, government and private practice.

- Throughout FY 2019, DOJ CHIP AUSAs presented at multiple China IP Road Shows across the U.S., sponsored by the USPTO. 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 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.

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.

Several years ago, NSD placed 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. Pursuant to this increased focus over the last several years, 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.

China Initiative

On November 1, 2018, former Attorney General Sessions announced the Department-wide China Initiative in order to emphasize the Department's strategic priority of countering Chinese national security threats, consistent with the Administration's national security strategy. The Initiative is comprised of the Assistant Attorney General (AAG) for National Security, the AAG for the Criminal Division, five United States Attorneys, and the Executive Assistant Director of the Federal Bureau of Investigation's (FBI's) National Security Branch, who collectively form the Initiative Steering Committee ("the Committee"). The AAG for National Security serves as Chair of the Committee.

The goal of the Initiative is to disrupt and deter Chinese "economic aggression," a government-sponsored effort that employs both licit and illicit tactics to obtain and transfer U.S. intellectual property for the benefit of Chinese commercial and military interests. To respond to Chinese economic aggression, the Initiative members were tasked with: (1) identifying priority economic espionage and trade secret theft cases, ensuring that the cases are adequately resourced, and bringing them to fruition in a timely manner, consistent with the facts and the law; (2) developing an enforcement strategy concerning Non-Traditional Collectors (i.e. researchers in labs, universities, government contractors, etc.) that are being coopted into transferring technology from the United States; (3) supporting outreach efforts by U.S. Attorney's offices throughout the country, to inform corporations and research institutions in their districts about the risk posed to U.S. intellectual property; (4) addressing supply chain and other threats to critical infrastructure, with a particular emphasis on telecommunications/5G, including by ensuring the effective implementation of the Foreign Investment Risk Review

Modernization Act of 2018; (5) disrupting soft power influence efforts on university campuses and elsewhere, both through the application of the Foreign Agents Registration Act, where feasible, and through outreach to civil society and academia; and (6) evaluating whether there is a need for additional legislative, administrative, law enforcement, or other tools to protect national assets.

(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 numerous 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 2019, listing the number of defendants and cases charged, the number of defendants sentenced, and the length of those sentences.[8] 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 2019
Investigative Matters Received by AUSAs	162
Defendants Charged	89
Cases Charged	57
Defendants Sentenced	55
No Prison Term	26
1-12 Months	14

[8] 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.

13-24 Months	4
25-36 Months	5
37-60 Months	5
60 + Months	1

In addition, the chart below details FY 2019 statistics for criminal IP cases broken down by type of charge.[9]

Charge	Cases charged	Percentage
Trademark *Trafficking in counterfeit goods, 18 U.S.C. § 2320*	31	48%
Copyright *Criminal copyright infringement, 17 U.S.C. § 506; 18 U.S.C. § 2319* *Counterfeit labels, 18 U.S.C. § 2318* *DMCA, 17 U.S.C. § 1201*	14 1 2	22% 2% 3%
Economic Espionage Act *Economic espionage, 18 U.S.C. § 1831* *Theft of trade secrets, 18 U.S.C. § 1832*	 2 14	 3% 22%
Total	**64**	**100%**

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

The Criminal Division currently devotes fourteen 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.

[9] 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.

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 ICHIP program (formerly known as 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 ICHIP 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 the ICHIP program in FY 2016 by posting new regional ICHIPs in Hong Kong and Sao Paolo, Brazil. In FY 2017, the State Department and DOJ prepared to field a new ICHIP position in Abuja, Nigeria. The Nigeria ICHIP deployed in October 2017. Most recently, in FY 2019, the State Department and DOJ added new regional ICHIP positions in Kuala Lumpur, Malaysia, and The Hague, Netherlands, two new ICHIP Advisors based in Washington, D.C. with the subject matter expertise in Global Dark Web and Cryptocurrency issues and Global Internet Based Fraud and Public Health issues, and a Global Cyber Forensic Advisor also based in Washington, D.C. In 2020, the ICHIP Network will expand to include regional ICHIPs in Panama City, Panama; Zagreb, Croatia; and Addis Ababa, Ethiopia. This will bring the total number of ICHIPs to twelve, plus one Global Cyber Forensic Advisor.

In addition to evaluating digital evidence, the CCIPS 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 four sections of the Department's Civil Division: the Intellectual Property Section, the National Courts Section, the Consumer Protection Branch, and the Civil Appellate Staff. 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. 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. Finally, the Civil Appellate Staff represents the United States in copyright and trademark cases in the courts of appeals, including participating as an amicus or intervenor in private IP litigation involving important government interests and defending

decisions of the Copyright Office and the U.S. Patent and Trademark Office against constitutional and statutory challenges.

(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 the National Cyber Investigative Joint Task Force 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

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
FDA	Food and Drug Administration
FBI's Annual Report	FBI Fiscal Year 2017 Report to Congress on Intellectual Property Enforcement
FSN	Foreign Service National
FTC	Federal Trade Commission
FY	Fiscal Year
ICE-HSI	Immigration and Customs Enforcement's Homeland Security Investigations
ICHIP	International Computer Hacking and Intellectual Property
IP	Intellectual property
IPR	Intellectual property rights
IPEC	Intellectual Property Enforcement Coordinator
IPEP	Intellectual Property Enforcement Program
IPLEC	Intellectual Property Law Enforcement Coordinator
IPR Center	National Intellectual Property Rights Coordination Center
NSCS	National Security Cyber Specialists
NSD	National Security Division
NW3C	National White Collar Crime Center
OIA	Office of International Affairs
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