United States Department of Justice

PRO IP Act
Annual Report FY 2020

PRO IP ACT ANNUAL REPORT OF THE ATTORNEY GENERAL FY 2020

INTRODUCTION

The Department of Justice (the "Department" or "DOJ")[1] submits this Fiscal Year 2020 ("FY 2020") 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 2020 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 2020 (*i.e.*, October 1, 2019, through September 30, 2020) are set forth below.

In addition, working closely with the Office of the Intellectual Property Enforcement Coordinator ("IPEC"), the Department contributes to strategic planning and implementation as well as the IPEC's annual reports.

(a)(1) State and Local Law Enforcement Grants

> *"(1) With respect to grants issued under Section 401, the number and identity of State and local law enforcement grant applicants, the number of grants issued, the dollar value of each grant, including a breakdown of such value showing how the recipient used the funds, the specific purpose of each grant, and the reports from recipients of the grants on the efficacy of the program supported by the grant. The Department of Justice shall use the information provided by the grant recipients to produce a statement for each individual grant. Such statement shall state whether each grantee has accomplished the purposes of the grant as established in Section 401(b). Those grantees not in compliance with the requirements of this title shall be subject, but not limited to, sanctions as described in the Financial Guide issued by the Office of Justice Programs at the Department of Justice."*

In FY 2020, 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, 2020 Pub. L. No. 116-93, 133 Stat. 2317, 2407, 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 2020, OJP was able to grant eight awards totaling $2,265,147 to local and state law enforcement and prosecutorial agencies. The following FY 2020 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
2020-H2150-CT-IP	City of Hartford	$399,545
2020-H2188-NC-IP	North Carolina Department of the Secretary of State	$125,000
2020-H2055-CA-IP	City of Los Angeles	$125,000
2020-H2180-TX-IP	City of Austin	$400,000
2020-H2193-CA-IP	County of Los Angeles	$399,080
2020-H2103-NJ-IP	State of New Jersey, Department of Law & Public Safety	$199,900
2020-H2164-TX-IP	City of Houston	$400,000
2020-H2123-LA-IP	Louisiana Department of Justice	$216,622

Since the inception of the program, OJP has awarded over $32.2 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 $25.2 million. Throughout the duration of the program, these agencies have made seizures totaling over $1.029 billion, which includes counterfeit merchandise and other property as well as currency.

During the one-year period July 1, 2019 – June 30, 2020, grantees reported seizures totaling **$70,249,205** (**$69,554,628** in counterfeit merchandise, **$560,196** in other property, and **$134,381** in currency). Over this same one-year period, grantees engaged in the following law enforcement activities:

- **204** individuals were arrested for violations of IP laws;
- **73** state and local IP search warrants were served; and
- **197** piracy/counterfeiting organizations were disrupted or dismantled.

Examples of how state and local law enforcement used prior IPEP grants in FY 2020 include:

- The City of Austin, TX IP Crime task force made significant progress in an on-going, lengthy investigation targeting the selling and possessing of counterfeit items, such as soccer jerseys. The operation included purchasing counterfeit items from the suspected person as well as the suspected place. Officers conducted

hours of surveillance to determine where the suspected person lived, where the suspected person was storing the counterfeit items, and where the suspected person was coming from. Officers also worked to submit the items of evidence in a professional manner to prepare for possible courtroom testimony. The detective assigned to the case began preparing a search warrant for the suspected place. Officers later executed the signed search warrant. Officers seized over $10,000 MSRP worth of counterfeit clothing items. The investigation is ongoing, and the task force members are also pursuing three different counterfeit leads that may lead to operations in the future.

- The Counterfeit and Piracy Enforcement team in Los Angeles County conducted counterfeit investigations resulting in multiple arrests, the dismantling of five counterfeit organizations, and the seizure of approximately 5,800 counterfeit products with an MSRP of over $5 million.

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, 2019, and September 30, 2020, NW3C conducted these training sessions for 398 attendees from 319 agencies. During this time, NW3C also conducted relevant IP webinars, training 1,802 attendees from 1,167 agencies. NW3C also continued to provide technical assistance to IPEP grantee task forces, as well as maintain and update asynchronous 24/7 online IP theft training.

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

- 121 IP theft trainings for 3,005 attendees from 1,612 agencies
- 18 seminars/webinars for 2,340 attendees from 1,352 agencies
- 785 attendees from 652 agencies successfully completed web-based training and utilized online resources specific to IP investigations
- 44 technical assistance meetings for 573 attendees from 135 agencies

NW3C continues to manage 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 contains legal resources for prosecutors and judges as well as resources for the general public.

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

- Chicago Police Department detectives attended NW3C Intellectual Property Rights ("IPR") training and, after the course, requested assistance from NW3C instructors in analyzing financial records and determining prosecutorial strategy. NW3C instructors guided the detectives through tracing and seizing bank accounts which resulted in identifying and filing felony charges against multiple suspects. The outcome of this case is pending.

- Detroit Police detectives conducting an investigation into IP theft contacted NW3C instructors and asked for subpoena templates for financial institutions. In addition to providing the templates, NW3C instructors explained how to set up a controlled buy, manage the large amount of evidence that accumulates in IPR cases, and establish contact with brand holders.

(a)(2) Additional Agents of FBI

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

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

(a)(3) FBI Training

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

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

(a)(4) Organized Crime Plan

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

As in FY 2009 through FY 2019, Congress did not appropriate funds to support Section 402(b) of the PRO IP Act in FY 2020.[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 2020, the Department has taken the following additional actions to address this important issue:

Increased Information Sharing and Coordination

The Department, through the Criminal Division, is continuing to coordinate with federal investigatory agencies to work with the International Organized Crime Intelligence and Operations Center in an ongoing effort to develop and implement a mechanism to 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 2020, 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

[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."

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. In FY 2020, funds were neither appropriated under this section nor expended based on funds previously appropriated under this section. Information about the cases, defendants, and types of investigations carried out by the Department may be found in greater detail below.

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

(a)(6) Other Relevant Information

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

The Department did not receive any authorizations under Sections 402 and 403 of the PRO IP Act in FY 2020.

(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 coordinated closely with the 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.

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-six 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

[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 2019 PRO IP Reports are available at the same location.

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 eight 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; São Paulo, 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 serve as global subject matter experts on dark web and cryptocurrency issues and internet-based fraud and public health issues; and a Global Cyber Forensic Advisor, also based in Washington, D.C. In 2020, the Network expanded 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

[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.

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 NSCS Network representatives have convened annually 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 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 federal law enforcement 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

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

[6] These federal agencies include Customs and Border Protection ("CBP"), the Federal Bureau of Investigation ("FBI"), the United States Postal Inspection Service ("USPIS"), the Food and Drug Administration's ("FDA") 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.

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 2020 both domestically and abroad. Some of these efforts are highlighted below:

Prosecution Initiatives

The Department continues to prioritize IP investigations and prosecutions that involve (1) health and safety, (2) trade secret theft or economic espionage, and (3) large-scale commercial counterfeiting and online piracy. The Department has also increased its focus on IP crimes that are committed or facilitated by use of the Internet or perpetrated by organized criminal networks.

(1) Health and Safety

The Department's health and safety initiative brings together private, state, and federal enforcement resources to address the proliferation of counterfeit goods posing a danger to consumers, including counterfeit and illegally prescribed pharmaceuticals, automotive parts, and military goods. In FY 2020, this initiative resulted in a number of significant prosecutions, including those set forth below:

- *Online Drug Dealer Sentenced to 15 Years for Distributing Counterfeit Pills Containing Fentanyl that Caused Overdose Death.* On October 16, 2019, Trevon Antone Lucas was sentenced to 15 years in federal prison for selling counterfeit oxycodone pills containing deadly fentanyl that caused the overdose death of a La Jolla resident in June of 2018. Lucas, a resident of Highland, California, pleaded guilty in June 2019 to distribution of fentanyl resulting in death. In his plea, he admitted that he posted online advertisements for the illegal sale of prescription pills. The investigation revealed that Lucas was warned about the danger of the pills he was selling on two separate occasions. In late 2017, Lucas was warned that the pills he was selling were counterfeit and contained fentanyl that was much stronger than oxycodone pills. Then, just two months prior to the victim's death in mid-2018, Lucas was explicitly warned that counterfeit pills containing fentanyl had caused the overdose of a San Diego resident. Lucas continued to sell the counterfeit pills. According to Lucas' plea agreement, on the evening of June 29, 2018, Lucas met the victim and sold him nine "blues," a slang term for prescription oxycodone pills. The "blues" Lucas sold were counterfeit and contained fentanyl—the same pills that Lucas had previously been warned about selling. The victim died after consuming the pills. Three other individuals were charged in the same indictment with conspiring with Lucas to distribute prescription hydrocodone pills; all three have since pleaded guilty and been sentenced.

- *Large-Scale Counterfeit Fentanyl Pill Dealer Sentenced to 30 Years in Prison.* On October 31, 2019, Dion Gregory Fisher was sentenced to 30 years in federal prison for

money laundering and conspiracy to manufacture and distribute fentanyl and fentanyl analogue. Fisher was ordered to forfeit several high-end vehicles, and a forfeiture money order of nearly $800,000 was entered against him. A federal jury had found Fisher guilty on June 5, 2019. Testimony and evidence presented during the seven-day trial showed that Fisher and others, including co-defendant Christopher McKinney, manufactured and distributed hundreds of thousands of counterfeit oxycodone 30 mg pills that were made with fentanyl that Fisher had ordered from China. The government admitted into evidence more than three kilograms of fentanyl and fentanyl analogue. On July 2, 2018, McKinney pleaded guilty to conspiring to distribute and manufacture fentanyl and fentanyl analogue, and he forfeited $1.4 million in cash, two residences, and several high-end vehicles and a motorcycle. Fisher and McKinney sold hundreds of thousands of counterfeit oxycodone pills, mostly via the U.S. Mail, to Phil Morose in Boston. Morose then distributed the pills. Morose was charged with conspiring to distribute and manufacture fentanyl and fentanyl analogue. He pleaded guilty to these charges and was sentenced on July 8, 2019, to 10 years in federal prison.

- *East Bay Men Charged with Selling Counterfeit Pills Laced with Fentanyl.* On December 12, 2019, Jose Ricardo Loza and Randy Lee Walker were arrested and charged with distributing fentanyl and heroin. When law enforcement agents arrested Loza, they found more than 2,000 counterfeit oxycodone pills hidden in hollowed out compartments of his furniture. An affidavit filed in the case alleges that Loza sold blue counterfeit oxycodone pills laced with fentanyl. According to the affidavit, Loza sold to a third party 50 fentanyl-laced pills on August 22, 2019, when at the auto body shop where he worked in Pittsburg, California. Loza allegedly did not initially have enough pills to sell, so he texted Walker, who arrived with more fentanyl-laced pills. During the transaction, Loza allegedly warned the customer to be careful because he (Loza) gave the same pills to a mutual friend who overdosed and died. The affidavit also alleges that on November 22, 2019, Loza sold 500 more counterfeit pills to an undercover officer and told the officer that he had 10,000 more of the same pills for sale, and on September 10, 2019, Loza sold two ounces of heroin.

- *Champaign Man Sentenced to 13 Years in Prison for Trafficking Millions of Counterfeit Xanax Pills on Darknet, Money Laundering.* On January 6, 2020, Stephan Caamano, a Champaign, Ill., man, was sentenced to 13 years in federal prison for trafficking at least 4.3 million counterfeit Xanax pills throughout the country and laundering the proceeds. Caamano has been ordered to pay more than $2.1 million he gained in profits through this scheme and to serve a three-year term of supervised release upon completion of his prison sentence. On April 29, 2019, Caamano pleaded guilty to using darknet markets and cryptocurrency to traffic pills containing alprazolam, marked as ‘Xanax,’ from March 2017 through May 2018. Caamano purchased controlled substances from abroad to make the counterfeit pills. The pills were manufactured to appear identical to prescription Xanax. Caamano then shipped the pills nationwide in quantities ranging from 1,000 pills per package up to one million.

- *Philadelphia Man Sentenced to 20 Years in Prison for Trafficking Counterfeit Drugs that He Purchased on Dark Web with Bitcoin.* On March 10, 2020, Michael Gordon, of

Philadelphia, was sentenced to 20 years in federal prison, followed by three years of supervised release, for conspiracy to traffic in counterfeit goods and conspiracy to commit money laundering. The Court further ordered Gordon to pay over $2.7 million in restitution and to forfeit over $300,000. From approximately December 2017 until October 2018, Gordon was involved in a sophisticated scheme to obtain counterfeit Xanax on the dark web and to sell the counterfeit pills for a profit. He took numerous steps to conceal his illegal activity, such as having packages mailed to fictitious recipients at a variety of locations that Gordon himself controlled. Additionally, he paid for the counterfeit pills using Bitcoin, re-sold the counterfeit pills for a profit, and then laundered the proceeds of his illicit drug business to conceal the true nature of the funds. Before law enforcement stopped Gordon, he illegally obtained and redistributed hundreds of thousands of these counterfeit pills. He pleaded guilty to the charges in June 2019.

- *Ukrainian Men Plead Guilty to Conspiracy and Trafficking Counterfeit Cancer and Hepatitis Drugs.* On July 17, 2020, two Ukrainian citizens admitted to conspiring to smuggle and distribute counterfeit cancer and hepatitis drugs into the United States. Maksym Nienadov, the owner of the Ukrainian-based company Healthy Nation, and his co-conspirator and employee, Volodymyr Nikolaienko, pleaded guilty to conspiracy, trafficking in counterfeit drugs, and smuggling goods into the United States. Nienadov also admitted to introducing misbranded medicine into the United States. Neither Nienadov nor Nikolaienko are medical doctors, pharmacists, or licensed pharmaceutical wholesalers in the U.S. and neither had authorization to sell the drugs. Beginning in June 2018, undercover U.S. authorities began communicating with the two men and facilitating undercover purchases. Nienadov and Nikolaienko were taken into custody on April 18, 2019, after they arrived in the U.S from Ukraine to discuss future unlawful shipments of pharmaceuticals.

- *Manufacturing Broker Pleads Guilty in Conspiracy to Manufacture and Sell Counterfeit Goods.* On August 25, 2020, Bernard Klein, a New York businessman, pleaded guilty to conspiracy to commit mail fraud and admitted that he conspired with New York wholesaler Ramin Kohanbash, 50, and at least one other person, to arrange the mass production of goods in China and Pakistan that carried counterfeit markings and labels identical to genuine trademarks registered with the U.S. Patent and Trademark Office. Some of the counterfeit items were distributed to members of the United States military. Klein facilitated the manufacturing of goods that contained the counterfeit markings. According to information presented to the court, Klein and Kohanbash instructed the manufacturers on how to fold and package the counterfeit goods, and to affix removable "Made in China" stickers to avoid problems when U.S. Customs inspected shipments. On June 13, 2019, Kohanbash pleaded guilty to conspiracy to commit wire fraud and trafficking in counterfeit goods, and he admitted that among the items he and others arranged to counterfeit were 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.

- *Husband and Wife Plead Guilty to Naturalization Fraud and Conspiring to Illegally Import and Distribute Male-Enhancement Products and Counterfeit Goods from China.* On September 24, 2020, Irfanali Momin and Shiba I. Momin a/k/a Saguftabanu Momin, husband and wife, each pleaded guilty to naturalization fraud, and conspiring to illegally import misbranded drug products from China, receive misbranded drugs that had moved in interstate commerce, and to trafficking of counterfeit goods. According to the prosecution, the charges, and other information presented in court, between August 2014 and November 2018, the Momins ordered and sold male-enhancement products from China marketed under names such as "Black Ant King," "Bull," "Rhino 7," and "Black Mamba." These products contained sildenafil, the active pharmaceutical ingredient in Viagra, and/or tadalafil, the active pharmaceutical ingredient in Cialis. Both Viagra and Cialis can be obtained in the U.S. only with a prescription from a doctor. The Momins admitted to selling between $550,000 and $1.5 million in illegal drug products over the course of the conspiracy. They also sold various counterfeit goods from their warehouse in Dalton, Georgia, including counterfeit designer watches, headphones, e-cigarette devices, and tobacco rolling papers.

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

In FY 2020, 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:

- *Chinese National Who Worked at Monsanto Indicted on Economic Espionage Charges.* On November 21, 2019, Haitao Xiang, formerly of Chesterfield, Missouri, was indicted by a federal grand jury on one count of conspiracy to commit economic espionage, three counts of economic espionage, one count of conspiracy to commit theft of trade secrets, and three counts of theft of trade secrets. According to the indictment, Xiang was employed by Monsanto and its subsidiary, The Climate Corporation, from 2008 to 2017, where he worked as an imaging scientist. Monsanto and The Climate Corporation developed a digital, on-line farming software platform that was used by farmers to collect, store, and visualize critical agricultural field data and increase and improve agricultural productivity for farmers. A critical component to the platform was a proprietary predictive algorithm referred to as the Nutrient Optimizer, which Monsanto and The Climate Corporation considered a valuable trade secret and their intellectual property. In June 2017, the day after leaving employment with Monsanto and The Climate Corporation, Xiang bought a one-way plane ticket to China. Before he could board his flight, federal officials intercepted Xiang at the airport and seized copies of the Nutrient Optimizer.

- *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage, and Wire Fraud for Hacking into Credit Reporting Agency Equifax.* On February 10, 2020, a federal grand jury returned an indictment charging four members of the Chinese People's Liberation Army with hacking into the computer systems of the credit reporting agency

Equifax and stealing Americans' personal data and Equifax's valuable trade secrets. The nine-count indictment alleges that Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei were members of the People's Liberation Army's 54th Research Institute, a component of the Chinese military. They allegedly conspired to hack into Equifax's computer networks, maintain unauthorized access to those computers, and steal sensitive, personally identifiable information of approximately 145 million American victims. According to the charges, the defendants exploited a vulnerability in the Apache Struts Web Framework software used by Equifax's online dispute portal. They used this access to conduct reconnaissance of Equifax's online dispute portal and to obtain login credentials that could be used to further navigate Equifax's network. The defendants spent several weeks running queries to identify Equifax's database structure and searching for sensitive, personally identifiable information within Equifax's system. The conspirators ultimately were able to download and exfiltrate the data from Equifax's network to computers outside the U.S. In total, the attackers obtained names, birth dates, and social security numbers for nearly half of all American citizens. The indictment also charges the defendants with stealing trade secret information, namely Equifax's data compilations and database designs. The defendants routed traffic through approximately 34 servers located in nearly 20 countries to obfuscate their true location, used encrypted communication channels within Equifax's network to blend in with normal network activity, and deleted compressed files and wiped log files on a daily basis in an effort to eliminate records of their activity.

- *Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research.* On July 7, 2020, a federal grand jury in Washington returned an 11-count indictment charging Li Xiaoyu and Dong Jiazhi, both nationals and residents of China, with hacking into the computer systems of hundreds of victim companies, governments, non-governmental organizations, and individual dissidents, clergy, and democratic and human rights activists in the U.S. and abroad. The defendants in some instances acted for their own personal financial gain, and in others for the benefit of the Ministry of State Security or other Chinese government agencies. The hackers stole terabytes of data which comprised a sophisticated and prolific threat to U.S. networks. The indictment alleges that Xiaoyu and Jiazhi, who were trained in computer applications technologies at the same Chinese university, conducted a hacking campaign that began more than ten years ago and lasted until the present, targeting companies in countries with high technology industries. Targeted industries included high-tech manufacturing; medical device, civil, and industrial engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense. More recently, the defendants probed for vulnerabilities in computer networks of companies developing COVID-19 vaccines, testing technology, and treatments.

- *Researcher Pleaded Guilty to Conspiring to Steal Scientific Trade Secrets from Ohio Children's Hospital to Sell in China.* On July 30, 2020, former Ohio woman Li Chen pleaded guilty to conspiring to steal scientific trade secrets and conspiring to commit wire fraud concerning the research, identification, and treatment of a range of pediatric medical conditions. Chen admitted to stealing scientific trade secrets related to exosomes

and exosome isolation from Nationwide Children's Hospital's Research Institute for her own personal financial gain. Chen worked in a medical research lab at the Research Institute for 10 years, from 2008 until 2018. According to her plea agreement, Chen conspired to steal and then monetize one of the trade secrets by creating and selling exosome "isolation kits." Chen admitted to starting a company in China to sell the kits. Chen received benefits from the Chinese government, including the State Administration of Foreign Expert Affairs and the National Natural Science Foundation of China. Chen also applied to multiple Chinese government talent plans, a method used by China to transfer foreign research and technology to the Chinese government. As part of her plea, Chen has agreed to forfeit approximately $1.4 million, 500,000 shares of common stock of Avalon GloboCare Corp., and 400 shares of common stock of GenExosome Technologies Inc.

- *Former Uber Executive Sentenced to 18 Months in Jail for Trade Secret Theft from Google.* On August 4, 2020, Anthony Scott Levandowski, of Marin County, California, pleaded guilty and was sentenced to 18 months in federal prison for trade secret theft related to Google's self-driving car program. Levandowski was also ordered to pay a $95,000 fine and $756,499.22 in restitution. Levandowski admitted that, from 2009 to 2016, he worked in Google's self-driving car program, known then as Project Chauffer. Levandowski admitted that, during this time, he was aware his employment agreement required him to keep Google's valuable non-public information confidential. He also admitted knowing that the non-public information related to Project Chauffeur was sensitive and subject to the confidentiality requirement. Nevertheless, in 2016, as he was preparing to leave Google, he downloaded onto his personal laptop thousands of Project Chauffer files and a variety of files from a corporate Google Drive repository. Among these files was an internal tracking document entitled "Chauffeur TL weekly updates – Q4 2015." The update contained a variety of confidential details regarding the status of Project Chauffer. Levandowski admitted he downloaded this file with the intent to use it to benefit himself and Uber Technologies, Inc. As part of his plea agreement, Levandowski admitted that the stolen document was Google's trade secret, and that a reasonable estimate of the loss attributable to his theft was up to $1,500,000.

- *One American and One Chinese National Indicted in Tennessee for Conspiracy to Commit Theft of Trade Secrets and Wire Fraud.* On August 4, 2020, a grand jury returned a superseding indictment, adding one count of conspiracy to commit economic espionage and one substantive count of economic espionage to a February 12, 2019, indictment against Xiaorong You, a/k/a Shannon You, of Lansing, Michigan, and Liu Xiangchen, of Shandong Province, China. You and Xiangchen were originally 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. A jury trial is scheduled to begin on April 6, 2021.

- *Chinese Citizen Sentenced for Economic Espionage, Theft of Trade Secrets, and Conspiracy.* On August 31, 2020, Hao Zhang, of China, was sentenced to 18 months in

federal prison and ordered to pay $476,835 in restitution following his conviction at trial on charges of economic espionage, theft of trade secrets, and conspiring to commit both offenses. Evidence submitted during the course of the four-day bench trial demonstrated that, from 2010 to 2015, Zhang conspired to and did steal trade secrets from two companies: Avago, a designer, developer, and global supplier of a broad range of analog, digital, mixed signal, and optoelectronics components and subsystems with a focus in semiconductor design and processing, headquartered in San Jose, California, and Singapore; and Skyworks, an innovator of high performance analog semiconductors headquartered in Woburn, Massachusetts. The district court found that Zhang intended to steal the trade secrets for the benefit of China. Evidence further showed that, in October 2006, Zhang and his co-conspirators started a business in China to compete with Avago and Skyworks. Zhang and Wei Pang, one of Zhang's co-conspirators, illicitly shared trade secrets with each other and with co-conspirators in China while they worked for the U.S. companies. Zhang and Pang then connected their venture to Tianjin University ("TJU") in China, an instrumentality of the Chinese government. By 2009, they left their work in the U.S. to relocate to China, following a plan laid out by TJU officials to form another company, Novana, in the Cayman Islands. During that time, Zhang obtained patents in his own name using trade secret information stolen from Avago. Additional evidence demonstrated that Zhang engaged in economic espionage to help TJU and Zhang's Chinese company unfairly compete in the multi-billion dollar global market for cell phone RF filters.

(3) Large-Scale Commercial Counterfeiting and Online Piracy

The Department continues to pursue significant, large-scale piracy and counterfeiting operations. In FY 2020, the Department has had a number of significant prosecutions, including those set forth below:

- *Federal Jury Convicts Former Video Store Owner of Selling Counterfeit DVDs.* On October 29, 2019, Douglas Gordon was convicted of mail fraud and two counts of copyright infringement following a seven-day jury trial. According to evidence presented at trial, Gordon, the former owner of a chain of video rental stores in eastern Maine, operated three websites from which he made more than $640,000 from sales of over 48,000 counterfeit copies of copyright-protected motion pictures. Representatives of MGM, CBS, Disney, Mercury Pictures, and other copyright owners testified that Gordon did not have permission to reproduce and distribute the movies. A senior investigator employed by the Motion Picture Association identified the DVDs as counterfeit. Based on undercover purchases made from the three websites, execution of search warrants, and forensic analysis of computers, investigators from ICE-HSI identified Gordon as the operator of the online businesses. A series of customers testified at trial that they expected, based on website advertisements, to receive authorized DVD movies with cover art and a plastic case but instead received a paper envelope with nothing more than a burned disc with a laser-etched movie title. Several of Gordon's former video store employees also provided evidence of his unlawful reproduction.

- *Newport Man Pleads Guilty to Copyright Infringement for Creating Illegal Video Streaming and Downloading Websites.* On November 25, 2019, Talon White, of Newport, Oregon, pleaded guilty to one count each of criminal copyright infringement and tax evasion. According to court documents, beginning in 2013, White engaged in a scheme to reproduce and distribute for sale thousands of copyrighted movies and television shows. To accomplish this, White set up numerous websites that hosted the infringing material. Members of the public purchased subscriptions to the websites and were able to stream or download the video content, including movies that had yet to be released to the public. In total, White's scheme netted more than $8 million. As part of the plea agreement, White agreed to pay $669,557 in restitution to the Motion Picture Association of America and $3,392,708 in restitution, including penalties and interest, to the IRS. White has also agreed to forfeit more than $3.9 million seized from his bank accounts, approximately $35,000 in cash, cryptocurrency holdings worth an estimated $424,000, and a 2,248-square-foot home in Newport, Oregon worth an estimated $415,000. These forfeitures are part of two related civil forfeiture cases in the District of Oregon and represent one of the largest civil forfeitures in the district's history. Sentencing is set for January 2021.

- *State Department Employee and Spouse Indicted for Trafficking in Counterfeit Goods from U.S. Embassy.* On December 18, 2019, a U.S. Department of State employee, Gene Leroy Thompson Jr., and his spouse, Guojiao "Becky" Zhang, were arrested for their role in an international conspiracy to traffic in counterfeit goods from the U.S. Embassy in Seoul, Korea. The couple were indicted by a grand jury in Eugene, Oregon, and charged with conspiracy and trafficking in counterfeit goods. According to the indictment and other court documents, from September 2017 through December 2019, Thompson Jr. and Zhang allegedly sold counterfeit Vera Bradley handbags from e-commerce accounts to persons throughout the United States. Thompson Jr., who is employed by the U.S. Department of State as an Information Programs Officer at the U.S. Embassy in Seoul, used his State Department computer to create accounts on a variety of e-commerce platforms, all from within a secure space within the Embassy. Once Thompson Jr. created these accounts, Zhang took primary responsibility for operating the accounts, communicating with customers, and procuring merchandise to be stored in the District of Oregon. Thompson Jr. and Zhang also directed a co-conspirator in the District of Oregon to ship items to purchasers across the United States.

- *Two New York Men, Members of Counterfeiting Ring, Sentenced to Years in Prison for Trafficking Fake Super Bowl and Other Game and Concert Tickets.* On February 28, 2020, Damon Daniels, of Bronx, New York, was sentenced to 24 months in federal prison and three years of supervised release for his participation in a conspiracy to produce and sell counterfeit tickets to sporting events and concerts. One co-defendant, Rahiem Watts, also of Bronx, New York, was sentenced the week prior to 41 months in federal prison and three years of supervised release for his role in the same scheme. Daniels pleaded guilty in September 2019 to charges including conspiracy to commit wire fraud, wire fraud, and conspiracy to traffic in counterfeit goods. The charges stem from the defendants' participation in a scheme with others to create counterfeit tickets to sporting events and concerts held in Philadelphia and throughout the country. Daniels and

Watts printed counterfeit tickets for events, sold the counterfeit tickets at various venues, and also distributed the counterfeit tickets to other sellers nationwide for resale to victims. The defendants and their associates advertised the fake tickets on websites like Craigslist, tricking unsuspecting fans into paying hundreds of dollars for fake tickets.

- *Three Defendants Each Sentenced to 46 Months for Trafficking Counterfeit DVDs.* On June 24, 2020, Hongtao Zhu, Hui Lin, and He Lin were each sentenced to 46 months in federal prison and required to pay $898,748.52 in restitution for trafficking in counterfeit DVDs. All three defendants pleaded guilty in October 2019, and admitted to conspiring to sell counterfeit DVDs, which were imported from China and sold via eBay, over a two-year period. The counterfeit DVDs appeared to be genuine Disney productions.

- *Chinese National Pleads Guilty to Federal Mail Fraud and Conspiracy Charges for Trafficking in Counterfeit Goods.* On July 10, 2020, Xiaoying Xu, a Chinese citizen residing in Covina, California, was sentenced to time served and restitution of $2.3 million after pleading guilty in December 2019 to federal conspiracy and mail fraud charges related to her trafficking in counterfeit goods. According to her plea agreement, from about August 2016 until approximately April 2019, Xu conspired with others to import and sell counterfeit consumer goods, specifically Pandora jewelry and Ray-Ban sunglasses. Xu used her residence and offices in El Monte and Alhambra, California, as destination points for shipments of counterfeit goods shipped from Hong Kong and China. Xu repackaged the counterfeit goods, then mailed them to unsuspecting customers throughout the U.S. who believed they had purchased authentic goods. Xu and other members of the conspiracy obtained funds from the victims of the counterfeit scheme through fraudulently acquired customer accounts opened in the names of other people at a global online payment company. The online payment company sent the victims' money to Xu by electronic transfer to bank accounts or by check, which Xu cashed at ATMs or deposited into bank accounts opened by co-conspirators. Xu admitted that, as a result of her fraudulent conduct and her knowledge of the fraudulent conduct of her co-conspirators, she sold $2,322,845 worth of counterfeit Pandora and Ray-Ban-branded products to unsuspecting customers, causing a loss to the customers of at least that amount. On April 24, 2019, Xu and Yiwen Zhu, a Chinese citizen and legal permanent resident of the U.S., were arrested and indicted on federal charges of conspiracy, mail fraud, and trafficking in counterfeit goods.

- *Acting U.S. Attorney Announces Federal Charges and International Operation to Dismantle Online Piracy Group.* On August 26, 2020, indictments were unsealed charging Umar Ahmad, George Bridi, and Jonatan Correa with copyright infringement. According to the indictments, from 2011 to the present, Ahmad, Bridi, Correa, and others known and unknown, were members of the Sparks Group, an international piracy group involved in illegally distributing movies and television shows on the Internet. The Sparks Group fraudulently obtained copyrighted DVDs and Blu-Ray discs from wholesale distributors in advance of their retail release date by, among other things, making various misrepresentations to the wholesale distributors concerning the reasons that they were obtaining the discs prior to the retail release date. Sparks Group members then used computers with specialized software to compromise the copyright protections on the

discs, a process referred to as "cracking" or "ripping," and to reproduce and encode the content in a format that could be easily copied and disseminated over the Internet. They uploaded copies of the copyrighted content onto servers the Sparks Group controlled, and other members further reproduced and disseminated the content on streaming websites, peer-to-peer networks, torrent networks, and other servers accessible to the public. The Sparks Group identified its reproductions by encoding the filenames of reproduced copyrighted content with distinctive tags, and also uploaded photographs of the discs in their original packaging to demonstrate that the reproduced content originated from authentic DVDs and Blu-Ray discs. Ahmad and Bridid arranged for discs to be delivered from distributors located in Manhattan, Brooklyn, and New Jersey to other members of the Sparks Group, including Correa, prior to their official release date. Ahmad, Bridi, and Correa then reproduced, and aided and abetted the reproduction of, these discs by using computer software that circumvented copyright protections on the discs and reproducing the copyrighted content for distribution on the Internet. The Sparks Group has caused tens of millions of dollars in losses to film production studios.

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 2019, approximately 100 prosecutors and law enforcement agents from around the country attended the National Advocacy Center's Economic Espionage and Trade Secrets Seminar. Presenters included CCIPS attorneys and the CCIPS Cybercrime Lab Deputy Director.

- In February 2020, CCIPS hosted its annual conference and training for CHIPs at the National Advocacy Center in Columbia, South Carolina. Prosecutors from U.S. Attorneys' Offices and Main Justice components who have been designated as a CHIP for their office attended. Instructors addressed the latest information and guidance with respect to the collection and use of electronic evidence, computer crime, intellectual property crime, and related issues. It also provided opportunities for CHIPs to form new relationships and strengthen existing relationships with their colleagues, which in turn improves national and international cooperation on cybercrime and IP matters. Over 100 CHIP prosecutors attended the three-day conference, which was also livestreamed on JTN.

- In May 2020, CCIPS provided virtual training for the Central District of California U.S. Attorney's Office on IP crimes and the statutes used to prosecute these offenses.

- In June 2020, CCIPS provided virtual training for the Northern District of Indiana U.S. Attorney's Office on IP crimes and the statutes used to prosecute these offenses.

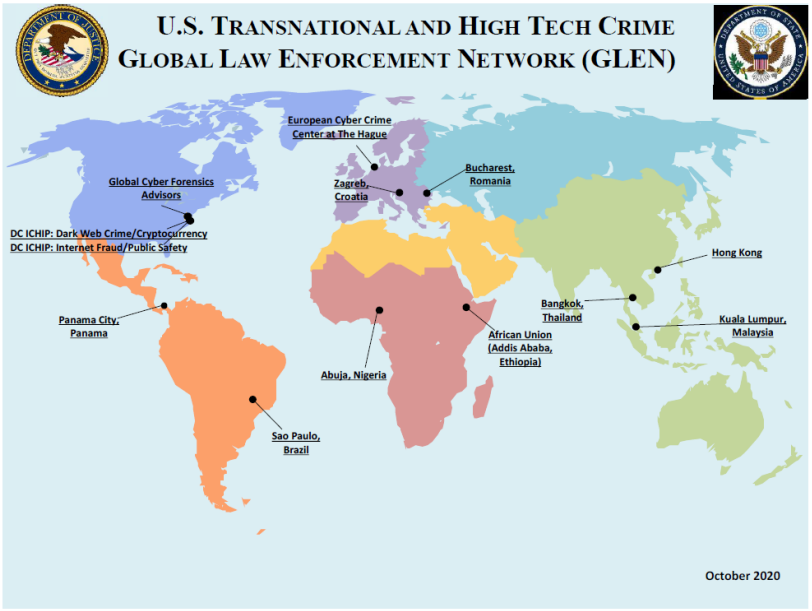
- In July 2020, CCIPS participated in a webinar series hosted by ICE-HSI's IPR Center. The series consisted of trainings and informational webinars related to the fight against counterfeit and fraudulent goods that have flooded markets during the COVID-19 crisis. CCIPS attorneys presented to a group of agents and attorneys on IP-related crimes.

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 constraints related to the COVID-19 pandemic, in FY 2020, 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 2020 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 2020, 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; São Paulo, 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 serve as global subject matter experts in dark web and cryptocurrency issues and 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 expanded to include regional ICHIPs based in Panama City, Panama; Zagreb, Croatia; and Addis Ababa, Ethiopia.[7]



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

ASIA

Programming on IPR Enforcement and Rule of Law in Myanmar. In October 2019, the Hong Kong ICHIP co-organized with OPDAT the Myanmar Resident Legal Advisor (a week of programming focused on IPR enforcement and rule of law in Yangon and Nay Pyi Taw, Myanmar. CCIPS representatives participated in a training workshop on IPR and transnational crime for prosecutors from the Union Attorney General's Office and other government officials in Myanmar. The workshop provided an overview of international illicit trade in counterfeit and pirated goods, best practices for investigation and prosecution of intellectual property crime, and basic digital forensics and online investigative tools. The assistance was timely given that Myanmar enacted comprehensive IPR legislation on trademarks, copyrights, patents, and industrial designs in 2019.

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

Workshops on IPR Crime in Vietnam and Ho Chi Minh City. From October to November 2019, the Hong Kong ICHIP conducted IPR criminal enforcement workshops for officials from the Ministry of Public Security and the Supreme People's Procuracy in Vietnam and Ho Chi Minh City. The U.S. Department of State Bureau of International Narcotics and Law Enforcement Affairs Hanoi office co-sponsored the training programs. 25 police and prosecutors attended each workshop. This was the fifth program the ICHIP led in Vietnam following Vietnam's revisions to its IPR criminal statutes in January 2018. The programs have provided guidance on issues raised by the newly amended legislation, such as fair and accurate valuation of infringing content and goods.

Presentation at Intellectual Property Enforcement Workshop for Prosecutors and Other Officials in Myanmar. In October 2019, CCIPS and its Cybercrime Lab participated in a training workshop on intellectual property rights and transnational crime for prosecutors from the Union Attorney General's Office and other government officials in Nay Pyi Taw, Myanmar. The workshop provided an overview of international illicit trade in counterfeit and pirated goods, best practices for investigation and prosecution of intellectual property crime, and basic digital forensics and online investigative tools. The workshop was organized by the Hong Kong-based ICHIP AttorneyAdvisor, with logistical support from OPDAT.

Instructed at Seminar on Combatting Smuggling. In November 2019, the Hong Kong ICHIP served as an instructor in Taipei, Taiwan, at a seminar for Taiwan Customs officers on combating smuggling. The seminar was jointly organized by Taiwan Customs and the ICE-HSI and CBP Attachés for Hong Kong, Macau, and Taiwan. The ICHIP presented on the steps customs officers can and should take when making seizures of IPR-infringing goods to assist criminal investigators and prosecutors in bringing strong cases. The agenda included sessions on passenger assessment in the U.S., a New Zealand Customs operations, a drug-smuggling case study, using express consignment services to combat smuggling, and a maritime drug interdiction.

Organized IPR Dialogues Between Vietnamese and U.S. Judges. In December 2019, the Hong Kong ICHIP staged IPR dialogues between Vietnamese and U.S. judges. Co-sponsors of the trainings were the Vietnam Supreme People's Court Judicial Academy, the USPTO Global Intellectual Property Academy, and the U.S. Embassy in Hanoi and U.S. Consulate in Ho Chi Minh City. 35 Vietnamese trial court judges attended each workshop. This was the sixth program the ICHIP staged in Vietnam to provide guidance on issues raised by Vietnam's January 2018 revisions to its IPR criminal statutes.

Planning Meetings for Amendments to Vietnam's Copyright, IP, and Trademark Statutes. In February 2020, the Hong Kong ICHIP traveled to Hanoi, Vietnam, to conduct planning meetings for a series of programs to assist the Vietnam Supreme People's Court in drafting and implementing guidance on 2018 amendments to the country's criminal copyright, industrial property, and trademark statutes.

Meeting with Malaysia's IP Representatives to Collaborate on IP Trainings. In June 2020, ICHIP representatives from Malaysia and Hong Kong held an online meeting with Malaysian

prosecutors attached to the Intellectual Property Section of Malaysia's Domestic Trade and Consumer Affairs Ministry. The meeting was held to discuss possible topics for webinars to be organized by the Malaysia and Hong Kong ICHIPs for the prosecutors, investigators and digital forensic analysts that investigate and prosecute IPR criminal violations in Malaysia. During the meeting, the chief prosecutor of the Intellectual Property Section stated that the section would be interested in participating in webinars focused on intellectual property offenses. She also stated that they were seeking to improve Malaysia's copyright law in order to tackle intellectual property theft via android boxes. The ICHIP representatives agreed to provide a list of possible online IPR crime and digital evidence topics that can be presented via webinars to Datuk Tay and their team for their review. They agreed to schedule the series of webinars in July.

Webinar Series on Enforcement Against COVID-19-Related Crimes. In June 2020, the Hong Kong ICHIP partnered with the ICHIP for Internet Fraud and Public Health ("IFPH"), the USPTO, and the Association of Southeast Nations Secretariat to present one in a series of webinars on enforcement against covid-19 crime: "Turning Consumer Complaints About COVID-19 Crimes into Criminal Enforcement." The webinar was viewed by 65 prosecutors, customs officers, regulatory officials, criminal investigators and IP rights holders' representatives from Brunei Darussalam, Cambodia, Fiji, Hong Kong, Indonesia, Japan, Malaysia, Myanmar, the Northern Mariana Islands, the Philippines, Singapore, Thailand, and Vietnam. The webinar included presentations on the interplay between consumer protection efforts and criminal enforcement and addressed a variety of major consumer protection issues arising during the COVID-19 pandemic: (i) fraudulent cure, treatment, protective, or testing products or services; (ii) price gouging on protective equipment and other consumer goods or services; (iii) contact tracing – privacy concerns and fraud concerns; (iv) refunds for canceled travel or events; (v) ensuring consumers receive relief payments; and (vi) mortgage services – protecting consumers' homes from foreclosure.

Webinar Series on IRP Criminal Enforcement. In July 2020, the Hong Kong ICHIP partnered with the Kuala Lumpur ICHIP to present a three-part series of webinars on IPR criminal enforcement to 32 prosecutors and 12 investigators from the Malaysia Attorney General's Chambers and the Malaysia Ministry of Domestic Trade and Consumer Affairs, respectively. The initial installment focused on turning border seizures of IPR-infringing goods into viable criminal investigations and prosecutions. The second presentation addressed best practices for combating online COVID-19 fraud, particularly the trafficking of counterfeit COVID cures. For the final installment, Datuk Tay of the Attorney General's Chambers pledged to continue the strong relationship established between the Attorney General's Chambers and the U.S. Department of Justice under the outgoing ICHIP in Kuala Lumpur with his successor. During this webinar, the Global Cyber Forensics Advisor ("GCFA"), who is also Director of DOJ's Cybercrime Laboratory, presented on best practices for the seizure, preservation and analysis of digital devices and evidence. The GCFA also urged criminal investigators and prosecutors to work closely and productively with digital crime analysts.

Webinar on IP Law Enforcement Issues in Pakistan and the U.S. In July, the Hong Kong ICHIP and CCIPS participated in a two-hour webinar, organized and chaired by USPTO, addressing intellectual property law enforcement issues confronted by officials from Pakistan and the United States. During the bilateral exchange, representatives from Pakistan's Directorate General of IPR

Enforcement described the IP enforcement issues facing their country. Officials from the U.S. CBP and the Office of the U.S. Trade Representative described IP enforcement issues that the United States is currently facing.

Webinar on IP Enforcement Coordination in the Philippines. In July 2020, the Hong Kong ICHIP presented at a webinar on IP enforcement coordination, organized jointly by USPTO's Global Intellectual Property Academy and the USPTO IP Attaché for Southeast Asia. Approximately 170 officials from the IP Office of the Philippines and the Philippines Department of Justice viewed the webinar. The Hong Kong ICHIP spoke to the participants about the ICHIP program and emphasized the common goals of the several U.S. federal agencies conducting IPR capacity-building activities in the Philippines and elsewhere in Asia.

Webinar on COVID Fraud and IP Crime Investigations for Sri Lankan Customs Officials. In August 2020, the Hong Kong ICHIP and the ICHIP for IFPH partnered with the Delhi-based USPTO Intellectual Property Attaché for South Asia to present a webinar entitled "Online Investigations of COVID-19 Frauds & Intellectual Property Crimes" to 50 officials from Sri Lanka Customs' specialized IPR Unit. The ICHIP for IFPH led the webinar, sharing best practices for investigating online COVID-19-related crimes and other fraud schemes, including IPR infringement. The ICHIP for IFPH also provided a comprehensive examination of the tools that investigators and prosecutors can use to follow the money in an online investigation in order to find the true identity of the criminal.

Webinar on IPR Enforcement in COVID-19-Era Dark-Web Marketplace. In August 2020, in partnership with the USPTO and the IP Office of the Philippines, the ICHIP for Dark Web and Cryptocurrency conducted a webinar entitled, "Prosecuting Dark Web Marketplace Administrators and Vendors" for over 182 officials from the IP Office of the Philippines, police, prosecutors, customs, and other IPR enforcement authorities. This was the third installment of a webinar series on IPR enforcement for Philippines officials. The goal of this virtual training series is to strengthen IPR enforcement against the sale of substandard, counterfeit, and IP-infringing products sold via dark-web marketplaces during the COVID-19 pandemic. At the end of the presentation, the participants engaged the ICHIP with over 30 minutes of questions and expressed interest in developing leads and opening investigations against dark-web vendors selling illegal and IP-infringing products.

NORTH AFRICA AND THE MIDDLE EAST

Presentation at IP Summit in Turkey. In October 2019, the Romania ICHIP team attended the "Summit on the Role of Intellectual Property in Promoting Creativity and Innovation for a Strong and Competitive National Economy" in Istanbul, Turkey, which was sponsored by the International Chamber of Commerce. Participants included business leaders, government officials, and members of academia. The ICHIP team gave a short presentation to 250–300 people on the challenges of IP theft and cybercrime, the role of the ICHIP, and DOJ's commitment to offering assistance on these issues.

Presentation on IPR Enforcement to Judges from the Kazakhstan Supreme Court and Interdistrict Economic Courts. In November 2019, CCIPS participated in a one-day program organized by the USPTO for eight judges and other officials from the Kazakhstan Supreme Court, as well as two judges from Kazakhstan's specialized interdistrict economic courts, one from Nur-Sultan, and one from Almaty. CCIPS addressed the investigation, prosecution, and adjudication of IP crimes in the U.S. and Kazakhstan. The American Bar Association organized the visit.

Webinar on IP Enforcement Issues Bringing Together Law Enforcement Officials from the Islamic Republic of Pakistan and from the United States. In July 2020, CCIPS participated in a two-hour webinar organized and chaired by the USPTO addressing IP law enforcement issues confronted by officials from Pakistan and the United States. Representatives from the Pakistan's Directorate General of Intellectual Property Rights Enforcement described the IP enforcement issues facing Pakistan. Representatives from U.S. CBP and from the Office of the U.S. Trade Representative described IP enforcement issues facing the United States.

Meeting with Head of New Saudi Arabia IP Agency. In August 2020, CCIPS participated in a videoconference with Yasser Adelbassi, the head of the new Saudi Authority for Intellectual Property. With colleagues from other U.S. agencies, a CCIPS representative answered questions from Mr. Adelbassi about how the U.S. regulates and enforces copyright on video-sharing platforms, video-on-demand sites, and through over-the-top media services. Mr. Adelbassi expressed a strong interest in setting up further discussions between the U.S. and Saudi Arabian law enforcement regarding how the kingdom can improve IPR enforcement.

CENTRAL AND SOUTH AMERICA

Presentation at International Anti-Counterfeiting Coalition Summit. In October 2019, the Brazil ICHIP and various ICHIP-mentored and trained police, prosecutors, and customs officials from around Latin America presented at the International Anti-Counterfeiting Coalition regional brand protection summit in Orlando, Florida. Approximately 250 law enforcement officials and U.S. and foreign rights-holders attended the program and shared best practices in the investigation of physical and online markets that distribute counterfeit goods and the criminal organizations that manufacture and export these products to the region. The Assistant Attorney General keynoted the conference and praises the work of the ICHIP-mentored São Paulo interagency group of municipal officials, police and customs officers, and U.S. rights-holders in tackling notorious markets. The program also marked the first time that ICHIP-mentored anti-piracy Civil Police chiefs from Rio de Janeiro, Minas Gerais, and São Paulo were at the same event and had an opportunity to meet and discuss possible collaboration on cases involving the manufacture and transportation of counterfeit goods across state lines.

Training for São Paulo Officials on Non-Criminal Enforcement for Counterfeit Storage and Distribution. In October 2019, the Brazil ICHIP trained approximately 50 judges, municipal officials, and U.S. rights-holders at a program organized by U.S. rights-holders in São Paulo on the use of non-criminal enforcement tools in the U.S. to hold the landlords of notorious markets liable for the actions of lessees who store and distribute counterfeit goods on their premises. The ICHIP highlighted key provisions of California law used by local authorities in Los Angeles to

obtain injunctive relief and monetary damages against the landlords of commercial premises used to manufacture, store, and/or distribute counterfeit goods. The ICHIP-mentored São Paulo interagency group of municipal officials, customs officers, civil police, and U.S. rights-holders are using similar civil enforcement tools to seize counterfeit goods from physical markets and shut them down indefinitely.

Presentation on Best Practices in IP Investigation and Prosecution in São Paulo. In November 2019, the ICHIP Staff Attorney presented to approximately 200 police and prosecutors on the ICHIP program and best practices in the investigation and prosecution of IP and cyber-enabled crime at programs in the Brazilian cities of São Luis and Teresina organized by the Regional Security Office at Consulate Recife. The programs were aimed at educating local law enforcement about available U.S. government resources for assistance with ongoing investigations and capacity-building initiatives.

Presentation at U.S. Patent and Trademark Office Regional Workshop on Combating Trafficking of Counterfeit Medicine. In December 2019, CCIPS presented at the U.S. Patent and Trademark Office Global Intellectual Property Academy's Regional Workshop on Combatting Trafficking of Medicine. Attendees were prosecutors, law enforcement, customs officers, and health care providers in Brazil, Peru, and Mexico. CCIPS' presentations focused on the criminal investigation and prosecution of counterfeit medicine and health and safety products in the United States and Latin America, building a case for criminal prosecution, and sentencing and asset forfeiture.

Presentation of Best Practices in Trademark Crime Investigation and Prosecution in São Paulo. In February 2020, the Brazil ICHIP trained approximately 80 São Paulo-based state and federal police, prosecutors, customs officers, and regulatory officials on best practices in the investigation and prosecution of complex trademark infringement crimes at physical markets. The program marked the first time the ICHIP provided a capacity-building workshop for the interagency group he helped create and that seized approximately 3,842 tons worth of counterfeit goods worth over $300 million USD from March 2017 through September 2019. Local law enforcement officials from New York and Los Angeles joined the ICHIP to share their experiences and insights dealing with physical markets in their cities and how they use a combination of civil and criminal enforcement statutes to combat piracy. U.S. rights-holders also held a trade fair displaying samples of genuine and fake merchandise commonly found in São Paulo's markets and provided tips on how to distinguish them and collaborate with industry on trademark investigators and prosecutions.

Presentation at U.S. Patent and Trademark Office Training on Copyright in the Digital Age. In February 2020, CCIPS presented at the USPTO Global Intellectual Property Academy's Copyright in the Digital Age: Supporting Authors, Artists, and the Creative Industries in Mexico City, Mexico. Attendees included prosecutors, law enforcement, and other government officials from Mexico. CCIPS' presentations focused on digital piracy-related issues, including enforcement challenges in the digital age, set-top boxes, emerging trends, camcording, and criminal penalties. Other topics presented included industry perspectives on the copyright landscape in Mexico, internet treaties and technological protection measures and rights management information, and the U.S. perspective on the role of service providers. CCIPS also

attended meetings with Mexican government officials and industry representatives to work on IP enforcement issues.

Organized Intellectual Property Workshop for Brazilian Law Enforcement. In February 2020, CCIPS, along with law enforcement officers from ICE-HSI, CBP, the New York Police Department, the Los Angeles Police Department, and the Los Angeles County District Attorney's Office, served as faculty at an IP workshop for Brazilian federal and military police, prosecutors, and Brazil-based IP rights holders in São Paulo, Brazil. Topics included criminal enforcement strategies, targeting of fraudulent importers, public-private collaboration, and civil remedies. The U.S. Consul General in São Paulo gave closing remarks. The Brazil ICHIP organized the workshop, with logistical support provided by OPDAT.

IPR Training for Central American and Caribbean Law Enforcement. In March 2020, the Brazil ICHIP trained approximately 40 police and prosecutors from around Central America and the Anglophone Caribbean at an IPR Center program in Punta Cana, Dominican Republic. The ICHIP shared multiple success stories from his time in Brazil as examples of how he could help counterparts build their capacity to investigate and prosecute IP crime involving the Internet or traditional marketplaces. He also shared examples of how to preserve and obtain electronic evidence from U.S. providers and social networks and situations in which the ICHIP program and CCIPS could assist them. Finally, he explained the GLEN and how the addition of new positions, including Panama, could facilitate more support for counterparts throughout the Western Hemisphere.

Presentation on Best Practices on Investigating Online COVID-19 Scams in São Paulo. In May 2020, the Brazil ICHIP mentored approximately 40 Brazilian prosecutors, police, and customs officers on best practices for investigating and taking down online COVID-19 scams at a Microsoft Teams program organized by the United Kingdom's IP Attaché in São Paulo. The ICHIP discussed emerging trends in the sale of counterfeit goods in São Paulo due to COVID-19, including the apparent uptick in online sales from retailers that leased space at notorious markets like Bras and 25 de março. The ICHIP said that counterparts need to prepare for a sustained migration by these vendors to online marketplaces as a hedge against a sustained lockdown or future waves of infection that minimize foot traffic at the physical malls. An ICHIP-mentored São Paulo state prosecutor who works on cyber-organized crime also presented during the program and explained that he had worked with Mercado Livre to take down approximately 6,000 suspect COVID-19-related postings. Their work also led Mercado Livre to ban approximately 1,000 sellers from the platform. The prosecutor thanked the ICHIP for his assistance with learning how to engage effectively with private industry on these scams. ICHIP-mentored Civil Police and Federal Customs officers also summarized their agencies' recent enforcement actions and echoed the ICHIP's assertion that the pandemic is likely to accelerate the evolution of São Paulo's notorious markets to an online environment.

Presentation on Investigations of Online Trademark and Copyright Infringement. In August 2020, the Brazil ICHIP presented on best practices in the investigation of online trademark and copyright infringement for approximately 34 Brazilian law enforcement officials and industry representatives. He emphasized the importance of public and private sector collaboration and trending issues, such as the use of digital commerce platforms to distribute counterfeit goods.

The program was organized by a former U.S. Department of State's International Visitor Leadership Program participant and key contact of the Consulate's Public Affairs Section.

Training on Best Practices for Investigating COVID-19 IP Crimes. In August 2020, the São Paulo ICHIP and the ICHIP for IFPH partnered with the USPTO Attachés in Mexico, Peru, and Brazil to train approximately 100 prosecutors, customs officials, and trademark examiners from Peru, Bolivia, Argentina, and Paraguay on best practices in the investigation of IP crimes related to COVID-19. The ICHIP for IFPH presented on best practices for working with U.S. registrars to take down online COVID-19 scams voluntarily. He outlined the use of open source tools to learn the domain registrar and how to formulate effective requests for assistance to U.S. registrars. He also reminded participants of the G7 24/7 Network and other potentially useful tools for international assistance in preserving electronic evidence when it is identified during an investigation.

EUROPE

Meeting with High-Level Delegation from Bulgaria on IP and Cyber Issues. In October 2019, CCIPS met in Washington, D.C., with eight high-level officials from Bulgaria on IP and cyber issues. Among other things, the Bulgarian delegation briefed CCIPS on the status of the implementation of various recommendations made by CCIPS attorneys and other U.S. government officials to improve IPR protection in Bulgaria. For example, Bulgaria greatly expanded the Cybercrime Department to 40 officers, with 12 dedicated specifically to online piracy, and recently carried out a massive signal piracy operation that involved over 70 cable channels (that case is being prosecuted in four different courts in Bulgaria). Bulgaria also updated and circulated a revised version of their IPR prosecution manual pursuant to an official order by the Prosecutor General and increased the number of IPR cases prosecuted from last year. The meeting included a lengthy discussion about ways Bulgaria can incorporate sampling techniques and seizure of domains into its Internet piracy investigations and prosecutions.

Meeting with Four Judges from Ukraine about IP Cases. In October 2019, CCIPS met in Washington, D.C., with four Ukrainian judges—one from the Ukrainian Supreme Court, one from an oblast commercial court, and two from district courts—regarding investigating, prosecuting, and adjudicating IP cases in the United States and Ukraine.

Meeting with Delegation from Europe regarding IPR Enforcement and Customs Issues. In January 2020, CCIPS met at the State Department in Washington, D.C., with a group of 14 European officials from 10 European Union countries. Topics included DOJ's efforts to increase IPR enforcement around the globe, working with countries to increase their capacity on IPR enforcement, and issues regarding express consignment and international mail shipments, particularly those involving purchases through e-commerce sites.

Participation in IP Conference in Croatia. In February 2020, the Bucharest ICHIP participated in Intellectual Property for the European Union in a World of Challenges Conference held in Zagreb, Croatia, during the Croatian Presidency of the Council of the European Union. During the conference, the ICHIP delivered a presentation entitled "Global Dimension and Challenges of Trade Secrets." The Director of the event highlighted the ICHIP presentation in her closing

remarks; one of the other speakers asked to co-present with the ICHIP in the future; and several participants asked if the ICHIP could present at future events, to include future European Union events and potential events in Croatia and Lithuania.

Webinar on COVID-19-Related IP Crimes for Romanian Law Enforcement. In April 2020, the Bucharest ICHIP program partnered with the International Criminal Police Organization ("INTERPOL") and the USPTO to conduct a webinar focused on COVID-19-related cyber and IP crimes for more than 60 Romanian prosecutors and law enforcement agents. The webinar was titled "United in Combatting IP and Cybercrime during the Covid-19 Pandemic" and included presentations by the ICHIP for IFPH; ICE-HSI, IPR Center; FDA; INTERPOL; Europol; and the Council of Europe. Presenters discussed cybercrimes, counterfeit and substandard goods, and other IP crimes being committed during the COVID-19 pandemic, as well as practical measures to take down websites used to perpetrate these offenses.

Webinars on Investigating and Prosecuting Digital Piracy Cases. In June 2020, the Bucharest ICHIP partnered with the Director of Content Protection & Enforcement at the International Federation of the Phonographic Industry, in London, United Kingdom, to conduct two webinars on Investigating and Prosecuting On-Line Digital Piracy Cases for 70 Romanian police and prosecutors. Officials from INTERPOL and the U.S. Embassy's Economic Section also attended. The webinars focused on basic and advanced topics in investigating and prosecuting on-line digital piracy. The webinars covered such topics as investigative frameworks for on-line digital piracy, collection and preservation of digital evidence, and open-source investigative tools. The ICHIP offered multiple demonstrations of useful tools and techniques for investigating online crimes.

Webinar on Open Sources Intelligence Tools for Investigating IP Crimes and Organized Crime. In July 2020, the Bucharest ICHIP partnered with INTERPOL, Underwriters Laboratories ("UL"), and OPDAT Resident Legal Advisors in Albania, Kosovo, North Macedonia, and Georgia, to host a webinar, entitled "Open Source Intelligence Tools: The Convergence of Investigating Intellectual Property Crime, Organized Crime, Human Trafficking, and Cybercrime." The webinar–the 17th the Bucharest ICHIP team has led–provided an audience of more than 285 prosecutors and police officials from Albania, Bulgaria, Croatia, Georgia, Kosovo, Moldova, North Macedonia and Romania with a comprehensive introduction to open source intelligence. INTERPOL, Europol, and Council of Europe representatives also attended. And opening remarks were given by the U.S. Ambassador, the Romanian Minister of Justice, a Deputy Assistant Attorney General, the Romanian General Prosecutor, and INTERPOL representatives. During the webinar, UL experts highlighted the latest in open source intelligence investigative tools, online marketplace strategies, website and research tools, social engineering and creation of fake undercover identities, and more generally on best practices for successful investigations using open source intelligence.

Virtual Presentation on Trade Secret Protection and Enforcement for Ukrainian Officials. In July 2020, the Bucharest ICHIP delivered a virtual presentation, along with CCIPS, on the prosecution of trade secret theft to a group of Ukrainian government officials. USPTO hosted the webinar, entitled "Trade Secret Protection and Enforcement," which included a presentation on civil trade secret protection by a USPTO Attorney.

Participation in Virtual Meeting with Senior Romanian Government Officials on Proposed IP Work Plan. In September 2020, CCIPS participated in a virtual meeting with almost 40 Romanian and U.S. government officials to discuss a proposed work plan for Romania on IP issues in connection with the interagency Special 301 process, which examines IPR enforcement and market access to right holders in countries around the world. The proposed work plan would require Romania to develop a national IP strategy, identify a specific plan and timetable to monitor and evaluate progress on IP protection and enforcement, draft and propose legislation to implement the national IP strategy, appoint a high-level coordinator to develop and implement the strategy, set enforcement benchmarks for IP cases, and adopt a number of other specific reforms and improvements. CCIPS drafted part of the plan and suggested several provisions. During the meeting, Romania agreed to proceed with finalizing the details of the work plan by the end of 2020.

SUB-SAHARAN AFRICA

Participation in 13th Annual International Law Enforcement IP Crime Conference in Cape Town. In October 2019, CCIPS and ICHIPs, including the Abuja ICHIP, attended and participated in the 13th Annual International Law Enforcement IP Crime Conference in Cape Town, South Africa. The Abuja ICHIP presented at the Conference, and CCIPS and the ICHIPs took part in meetings with industry representatives during which the private sector shared information, concerns, and trends with the ICHIPs.

Hosted Second FANCAP Meeting in Nigeria. In November 2019, the Africa ICHIP team hosted the second Federal Agencies Network against Counterfeiting and Piracy meeting with representatives from numerous Nigerian agencies. The ICHIP Team is working with a network of agencies within Nigeria to establish a comprehensive plan of action to enhance IP protection, management, and enforcement.

Participation in World Intellectual Property Organization IP Program in Ethiopia. In December 2019, the Abuja ICHIP spoke at an IP program, sponsored by the World Intellectual Property Organization, jointly with the Ethiopian Intellectual Property Office in Addis Ababa, Ethiopia. The delegates at this national workshop on Building Respect for IP included law enforcement officials, members of the judiciary, and attorneys. In addition to the ICHIP, government speakers included a Senior FBI agent assigned to the IPR Center, an IP prosecutor from Romania, and a retired judge from South Africa. Private sector speakers included a representative from the International Trademark Association and Syngenta. The program also included several Ethiopian presenters to discuss its IPR regime.

Working Group on Pharma Crime. In December 2019, the Africa ICHIP Team led the second quarterly pharma-crime working group roundtable meeting. The working group members include prosecutors; customs officials; and investigators from Ghana, Botswana, Zambia, Kenya, Malawi, Namibia, Tanzania, Rwanda, Uganda, Nigeria, Liberia, Sierra Leone, and The Gambia. At this meeting, they discussed several trending matters, many of which arose during group communications via the WhatsApp platform set up at the first meeting in September 2019.

First Africa Pharma-Crime Working Group in Ghana. In March 2020, the ICHIP team convened the first meeting of the Francophone Africa Pharma Crime Working Group at the U.S. Department of State Bureau of International Narcotics and Law Enforcement Affairs Regional Training Center in Accra, Ghana. This meeting launched a pre-selected group of customs officers, regulators, investigators, and prosecutors drawn mostly from motivated alumni of ICHIP-led pharma-crime workshops in Accra, Ghana in August 2018 and in Dakar, Senegal in June 2019. Working group members came from Benin, Togo, Niger, Burkina Faso, Burundi, Republic of Congo, Côte d'Ivoire, the Democratic Republic of the Congo, Gabon, Guinea, Mali, Morocco, Chad, and Senegal. The working group was created to facilitate seizures and the exchange of expertise in criminal IPR matters and cases for investigation, prosecution. The group also hopes to encourage regional coordination, focusing on counterfeit products found regionally (primarily pharmaceuticals, but also auto parts, electronics, and other products that adversely affect human health and safety). The substantive exchange of information among neighboring countries should improve seizures, investigations, and prosecutions by working collectively on common sets of issues.

Participation in Brandholder Anti-Counterfeiting Forum. In May 2020, the Africa ICHIP team participated virtually, via WebEx, in a Brandholder Anti-Counterfeiting Forum for American Chamber of Commerce in South Africa (AmCham), organized jointly by U.S. Embassy EconOff for Trade and Investment in Pretoria, South Africa, and the Pretoria AmCham. The meeting was aimed at providing information on U.S. government resources available to U.S. companies in Africa and served as an introduction to continental points of contact for coordinating and collaborating on anti-counterfeiting and IP enforcement efforts. The ICHIP discussed law enforcement collaboration along with efforts to build the capacity of institutions dedicated to enforcing IP rights and combatting cybercrimes.

Collaboration Between Business, Government, and Universities in Nigeria on World Anti-Counterfeiting Day. In June 2020, the Abuja ICHIP team collaborated with the Business Action to Stop Counterfeiting and Piracy of the International Chamber of Commerce, the American Business Council, and the Intellectual Property Club of the University of Ilorin, Nigeria, to create awareness about the impact of using counterfeit products. The Business Action to Stop Counterfeiting and Piracy created different posters that were shared online on social media sites by the ICHIP team and the other collaborators. The Abuja ICHIP team also collaborated with the American Business Council and the Anti-Counterfeiting Collaboration to organize a public webinar for World Anti-Counterfeit Day, where Nigerian government officials spoke alongside private-sector representatives.

Participation in USPTO-Hosted Webinar. In July 2020, the Abuja ICHIP participated in a USPTO-hosted webinar titled "Sub Saharan Africa USG IP Webinar" for U.S. government personnel. The webinar discussed trademark fundamentals including brand protection and protection from counterfeits.

Webinar Series on Common COVID-19 Fraud Schemes. In July 2020, the ICHIP for Dark Web and Cryptocurrency and the ICHIP for IFPH partnered with OPDAT's Ghana Resident Legal Advisor, with assistance from the West Africa Regional Training Center, in Accra, Ghana, to conduct the second in their webinar series for 30 prosecutors, investigators, and financial

analysts from Ghana, Nigeria, Sierra Leone, and The Gambia. This webinar focused on common COVID-19 fraud schemes designed to exploit fears arising from the global pandemic and techniques for how to investigate them. The ICHIP for IFPH, who led the webinar, focused on three COVID-19-related crimes: fake cures peddled over the Internet, counterfeit pharmaceuticals and personal protective equipment, and government benefits frauds. He provided examples for how law enforcement and prosecutors can use tools to help obtain evidence of attribution and of fraudulent intent.

Webinar Series and Working Group on Fighting Fraud and Fake Medicine during COVID-19. In July and August 2020, the Abuja ICHIP and the ICHIP for IFPH hosted webinars in the "Fighting Fraud & Fake Meds in the Time of COVID-19" series for the Anglophone Pharmacrime Working Group. Attendees included working group members from seven African countries (The Gambia, Ghana, Kenya, Namibia, Nigeria, Sierra Leone, and Uganda) , along with representatives from South Africa. The ICHIPs invited one of Nigeria's representatives, the Principal Legal Officer with Nigeria's National Agency for Food and Drug Administration and Control, to share Nigeria's challenges and successes with investigating and prosecuting individuals for fake COVID-19 cures and counterfeit pharmaceuticals. The official discussed a case concerning a recent nationwide agency sweep of unregistered hand sanitizers that resulted in an arrest. He also discussed a case involving an illegal manufacturing and distribution plant where officers from his agency recovered several counterfeit drugs along with labeling materials.

Mentoring Session on Online Frauds and IP Crimes. In August 2020, the Abuja ICHIP and the ICHIP for IFPH conducted an in-depth mentoring session about online frauds and IP crimes for members of the Francophone Working Group based on input regarding the types of frauds they are facing. Additionally, the working group member from Togo discussed his country's investigative landscape and challenges, including using the Internet on cell phones to commit crimes.

Webinar Series on Fighting Counterfeit Pharmaceuticals. In August 2020, the Abuja ICHIP and the ICHIP for IFPH presented webinars titled, "Fighting Counterfeit Pharmaceuticals: A Case Study, Part One," and "Fighting Counterfeit Pharmaceuticals: A Case Study, Part Two." These webinars were their fifth and sixth in the "Fighting Frauds & Fake Meds in the Time of COVID" series. Attendees included working group members from eight African countries (Botswana, The Gambia, Ghana, Kenya, Namibia, Nigeria,, and Rwanda) and South Africa. The first webinar featured a criminal case demonstrating investigative and prosecutorial techniques discussed in the COVID-19 series, led by the ICHIP for IFPH and a Special Agent of the FDA Office of Criminal Investigations. Building on Part One's case study on counterfeit pharmaceuticals, FDA Special Operations Manager and the ICHIP for IFPH discussed how to attribute an online moniker to a real-world identity, as FDA investigators did in the featured criminal case. This led to a discussion about how member countries could use the G7 24/7 Network to preserve evidence as well as how non-members could join by talking with the Abuja ICHIP or the ICHIP for IFPH. The presenters discussed how obtaining electronic evidence can help not only with attribution, but also with proving intent and the identities of co-conspirators.

Webinar on Fighting Fraud & Fake Meds in the Time of COVID-19. In August 2020, the Abuja ICHIP and the ICHIP for IFPH hosted a webinar for Francophone African countries, the first in

the "Fighting Frauds & Fake Meds in the Time of COVID-19" series. The ICHIP for IFPH delivered a presentation focused on taking down fraudulent COVID-19 websites. This webinar included 14 participants from five countries: Chad, Burkina Faso, Burundi, Niger, , and Senegal. They highlighted fake chloroquine and fake sanitizer seizures at their borders and that those trafficking in these counterfeit products share information about them on social network platforms. Based on these discussions, the ICHIP for IFPH agreed to discuss online investigations at the next webinar.

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 2020, CCIPS organized and planned its Thirteenth Annual IP Industry and Law Enforcement Meeting held in Washington, D.C, in November 2019. The yearly meeting gives representatives from a broad range of industries 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 November 2019, in North Wales, Pennsylvania, CCIPS presented at the 2019 Merck Pharma Security Conference, titled "Insider Risk and Security Trends that threaten the US Pharma Industry." CCIPS' presentation covered aspects of trade-secret theft prosecutions and also included a case study of *U.S. v. Weiqiang Zhang*, a 2017 trade-secret-theft trial in Kansas about stolen bioengineered rice. Investigators, compliance personnel, and attorneys working with the pharmaceutical industry attended the conference.

- In November 2019, in Milwaukee, Wisconsin, CCIPS joined the FBI and Eastern and Western Districts of Wisconsin in a presentation on the department's China Initiative. Over 60 representatives from approximately 30 businesses throughout Wisconsin participated in the event. CCIPS addressed recent theft of trade secret prosecutions involving China and highlighted various ways to protect trade secret information during investigations and prosecutions.

- In December 2019, CCIPS spoke to over 100 government contracts managers and administrators at the Johns Hopkins University Applied Physics Laboratory in Laurel, Maryland about counterfeit and substandard military goods including electronic parts. CCIPS offered advice to employees about how to navigate the procurement

process to avoid buying counterfeit goods and what to do if they discover such goods in the supply chain. CCIPS also explained how DOJ and other agencies investigate and prosecute such cases, and how government-contracts personnel can assist these efforts.

- In December 2019, a CCIPS representative participated on a panel discussion at the Intellectual Property Rights Coordination Center's Digital Piracy Summit in Arlington, Virginia, speaking to over 100 law enforcement agents, government employees, and industry representatives. As part of his presentation, the CCIPS representative addressed issues and challenges facing law enforcement in enforcing copyright laws in cyberspace.

- In June 2020, CCIPS participated in a panel for the American Bar Association – Intellectual Property Section via WebEx to discuss "Countering the Counterfeiters," CCIPS' and the IPR Center's resources, points for collaboration, and enforcement-related training to in-house counsel and law firm attorneys.

- In July 2020, CCIPS joined representatives of CBP and ICE-HSI in a panel discussion hosted by the Center for Anti-Counterfeiting and Product Protection at Michigan State University. The virtual discussion reached an audience of more than 700 participants representing brand owners, government officials, and members of the academic community.

- In August 2020, CCIPS presented to a largely private sector audience as part of a virtual Intellectual Property Rights conference hosted by the FBI San Francisco Private Sector Engagement Squad as a webinar series. In one webinar, CCIPS joined representatives from the FBI and the Northern District of California U.S. Attorney's Office in a presentation entitled "Introduction to IPR," which addressed investigating and prosecuting IP offenses, with a focus on issues related to theft of trade secrets and best practices for law enforcement and industry cooperation. In another webinar, CCIPS presented on *United States v. Weiqiang, Zhang*, a theft of trade secrets case, with the CEO of the victim company.

- In September 2020, CCIPS presented on criminal copyright infringement for the U.S. Department of Commerce, International Trade Administration's virtual roadshow, STOPfakes.

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 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 focused 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 has 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 to emphasize the Department's strategic priority of countering Chinese national security threats, consistent with the Administration's national security strategy. The Initiative Steering Committee is led by the Assistant Attorney General for National Security as the Chair of the Committee and also includes the Assistant Attorney General for the Criminal Division, five United States Attorneys, and the Executive Assistant Director of the FBI's National Security Branch.

The goals of the Initiative are to: (1) identify priority trade secret theft cases, ensuring that investigations are adequately resourced, and working to bring them to fruition in a timely manner and according to the facts and applicable law; (2) develop an enforcement strategy concerning non-traditional collectors (e.g., researchers in labs, universities, universities and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests; (3) educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus; (4) apply the Foreign Agents Registration Act to unregistered agents seeking to advance China's political agenda, bringing enforcement actions when appropriate; (5) equip the nation's U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their Districts and support their outreach efforts; (6) implement the Foreign Investment Risk Review Modernization Act (FIRRMA) for DOJ (including by working with Treasury to develop regulations under the statute and prepare for increased workflow); (7) identify opportunities to better address supply chain threats, especially those impacting the telecommunications sector, prior to the transition to 5G networks; (8) identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses; (9) increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States; and (10) evaluate whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.

(a)(7)(C) Investigative and Prosecution Activity of the Department with Respect to IP Crimes

As the cases highlighted above show, 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 2020, 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 FBI's Annual Report, provided pursuant to Section 404(c) of the PRO IP Act, for an accounting of arrest statistics.

District Totals	FY 2020
Investigative Matters Received by AUSAs	167
Defendants Charged	65
Cases Charged	37
Defendants Sentenced	41
No Prison Term	16
1-12 Months	11
13-24 Months	4
25-36 Months	0
37-60 Months	6
60 + Months	4

In addition, the chart below details FY 2020 statistics for criminal IP cases broken down by type of charge.[9]

[8] Case statistics were compiled by the Executive Office for U.S. Attorney's ("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.

[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.

Charge	Cases charged	Percentage
Trademark *Trafficking in counterfeit goods, 18 U.S.C. § 2320*	23	61%
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*	 4 0 3	 10% 0% 8%
Economic Espionage Act *Economic espionage, 18 U.S.C. § 1831* *Theft of trade secrets, 18 U.S.C. § 1832*	 2 6	 5% 16%
Total	**38**	**100%**

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

The Criminal Division currently devotes 15 full-time attorneys, along with paralegals and support staff, in CCIPS to IP issues. CCIPS also provides substantial support to the IPR Center, assigning at least one attorney, and sometimes more, to help identify and de-conflict investigative leads, as well as develop and execute national enforcement initiatives.

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

Over the last year, more than 20 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 worked with the Department of State to post a DOJ attorney in Bucharest, Romania, beginning in 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 São Paulo, Brazil. In FY 2017, the State Department and DOJ prepared to field a new ICHIP position in Abuja, Nigeria, which was deployed in October 2017. In FY 2019, the State Department and DOJ added new regional

ICHIP positions in Kuala Lumpur, Malaysia, and The Hague, Netherlands, and two new ICHIP Advisors based in Washington, D.C. who have global subject matter expertise in dark web and cryptocurrency issues and internet-based fraud and public health issues, respectively. A Global Cyber Forensic Advisor is also based in Washington, D.C. In FY 2020, the ICHIP Network expanded to include regional ICHIPs in Panama City, Panama; Zagreb, Croatia; and Addis Ababa, Ethiopia. 12 ICHIP attorneys now serve in the Network, 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 the 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 USPTO 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
FY	Fiscal Year
ICE-HSI	Immigration and Customs Enforcement's Homeland Security Investigations
ICHIP	International Computer Hacking and Intellectual Property
IFPH	Internet Fraud and Public Health
INTERPOL	International Criminal Police Organization
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
OJP	Office of Justice Programs
OPDAT	Office of Overseas Prosecutorial Development, Assistance and Training

PRO IP Act	*Prioritizing Resources and Organization for Intellectual Property Act of 2008*
USPTO	U.S. Patent and Trademark Office