

United States Department of Justice

PRO IP Act Annual Report FY 2021



PRO IP ACT ANNUAL REPORT OF THE ATTORNEY GENERAL FY 2021

INTRODUCTION

The Department of Justice (the “Department” or “DOJ”)¹ submits this Fiscal Year 2021 (“FY 2021”) 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 2021 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 2021 (*i.e.*, October 1, 2020, through September 30, 2021) 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 2021, 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, 2021 Pub. L. No. 116-260, 134 Stat 1182, 1258, 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 such as 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 2021, OJP was able to grant five awards totaling \$2,232,164 to local and state law enforcement and prosecutorial agencies. The following FY 2021 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
15PBJA-21-GG-02814-INTE	Tulsa County District Attorney	\$400,000
15PBJA-21-GG-02815-INTE	North Carolina Department of the Secretary of State	\$400,000
15PBJA-21-GG-02812-INTE	City of Los Angeles	\$400,000
15PBJA-21-GG-02816-INTE	City of Portland	\$400,000
15PBJA-21-GG-02813-INTE	State of New Jersey, Department of Law & Public Safety	\$232,164

Since the inception of the program, OJP has awarded more than \$34.4 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 more than \$27.4 million. Throughout the duration of the program, these agencies have made seizures totaling more than \$1.226 billion, which includes counterfeit merchandise and other property as well as currency.

During the one-year period July 1, 2020 – June 30, 2021, grantees reported seizures totaling **\$197,631,130** (**\$192,857,508** in counterfeit merchandise, **\$3,678,623** in other property, and **\$1,094,999** in currency). Over this same one-year period, grantees engaged in the following law enforcement activities:

- **196** individuals were arrested for violations of IP laws;
- **145** state and local IP-related search warrants were served; and
- **168** piracy/counterfeiting organizations were disrupted or dismantled.

Examples of how state and local law enforcement used prior IPEP grants in FY 2021 include:

- The IP Crime Task Force in Austin, Texas, TX IP Crime continued work on an investigation in Kyle, Texas, related to counterfeit Louis Vuitton items. Hours of surveillance and an undercover purchase provided the evidence needed to obtain a residential search warrant for the target residence and the seizure of various items bearing counterfeit marks of Versace, YSL, Ray Ban, Michael Kors, Louis Vuitton, Gucci, Givenchy, Fendi, Christian Dior, Chanel, Cartier, Burberry, and Balenciaga with an MSRP value of \$373,213. The Task Force shared information with other law enforcement agencies, including law enforcement in Corpus Christi. Also, the research of one Task Force member resulted in an IP-related

investigation in San Marcos, Texas. During this investigation, Task Force members made multiple undercover purchases and conducted hours of surveillance and research resulting in a residential search warrant being executed on the target residence. Results of this search warrant included the seizure of counterfeit items with an MSRP of \$1,350,870. Additionally, the Task Force initiated an investigation of a boutique located in north Austin for the sale of counterfeit Louis Vuitton products. Other investigations include the discovery of four new targets based on work generated by a Task Force officer. These investigations continued into FY 2022.

- In March 2021, the Essex County Prosecutor's Office IP Unit executed a search warrant at a business in West Caldwell, New Jersey, resulting in seizure of approximately 173 counterfeit items (e.g., Louis Vuitton handbags) valued at approximately \$70,000, as well as several trademark counterfeiting charges against the owner of the business. The IP Unit continues to prosecute cases involving intellectual property violations, including an indicted case against two defendants for, among other offenses, trademark counterfeiting involving thousands of counterfeit electronic cigarette products.
- The City of St. Louis detectives continued their efforts to disrupt the distribution and sale of counterfeit merchandise. Detectives continued to expand the knowledge base of partners in the effective identification and reporting of counterfeit merchandise. Detectives also developed an increased working relationship with Customs and Border Patrol to track incoming shipments leading to the generation of more leads.

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, 2020, and September 30, 2021, NW3C conducted 14 training sessions for 345 attendees from 313 agencies. During this time, NW3C also conducted relevant IP webinars, training 992 attendees from 827 agencies. NW3C also continued to provide technical assistance to Intellectual Property Theft Enforcement Program (IPEP) Grantee task forces, as well as maintain and update asynchronous online IP Theft training.

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

- 135 IP theft trainings for 3,350 attendees from 1,925 agencies
- 21 seminars/webinars for 3,332 attendees from 2,179 agencies
- 1,131 attendees from 980 agencies successfully completed web-based training and utilized online resources specific to IP-related investigations
- 48 technical assistance meetings for 578 attendees from 139 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:

- Detectives from the Richmond, Virginia Police Department—who attended NW3C’s IPTT training—requested assistance on a case involving counterfeit e-cigarette products. The detectives and NW3C representatives attended multiple virtual meetings with brand representatives to assist them in identifying counterfeit products. Detectives then worked with brand representatives to make undercover buys, which resulted in the discovery and seizure of counterfeit merchandise. Both criminal and civil litigation is pending.
- NW3C instructors provided guidance and resources to the Chesterfield County Police Department in Virginia and Homeland Security Investigations (HSI) during the seizure of inbound fraudulent packages from overseas. NW3C provided investigators with contact information for brand holders of the counterfeit merchandise and subpoena templates for financial institutions. NW3C also assisted in the service of a cease-and-desist order served on the recipient of the counterfeit merchandise.

(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 2020, Congress did not appropriate funds to support Section 402(b) of the PRO IP Act in FY 2021.² 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 from other ongoing efforts.

In addition to the ongoing activities detailed in PRO IP Act Reports for fiscal years 2009 through 2021, 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 IP-related intelligence gaps, 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 2021, 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

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.”

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

(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 2021, 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 2021.

(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 for increasing criminal fines for organizational defendants who steal commercial trade secrets, and allowing 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 coordinated closely with the IPEC in addressing the Administration’s priorities on IP enforcement and implementing the IPEC’s 2020-2023 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 more than 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. Seventeen CCIPS attorneys are assigned to IP enforcement. These attorneys prosecute criminal cases, assist prosecutors and investigative agents in the field, and help develop and implement the Department’s overall IP enforcement strategy and legislative priorities. CCIPS attorneys are available to provide advice and guidance to agents and prosecutors on a 24/7 basis. CCIPS attorneys also provide training on criminal enforcement of IP laws to prosecutors and investigative agents both domestically and abroad.

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/criminal-ccips/ccips-documents-and-reports>. The Department’s FY 2010–FY 2020 PRO IP Reports are available at the same location.

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 (“IPLC”) 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; Panama City, Panama; Zagreb, Croatia; Addis Adaba, Ethiopia; and The Hague, Netherlands. The GLEN also now includes two ICHIPs based in the United States, to serve as global subject matter experts on dark web and cryptocurrency issues and internet-based fraud and public health issues; and Global Cyber Forensic Advisors, based in Washington, D.C.

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 coordinators. In addition, 25 United States Attorneys’ Offices have CHIP Units, with two or more CHIP attorneys.⁴ CHIP attorneys have four major areas of responsibility including: (1) prosecuting computer crime and IP offenses; (2) serving as the district’s legal counsel on matters relating to those offenses and the collection of electronic evidence; (3) training prosecutors and law enforcement personnel in the region; and (4) conducting public and industry outreach and awareness activities.

CES and the NSCS Network

Within NSD, CES—one of NSD’s principal litigating components—is responsible for coordinating and conducting investigations and prosecutions of a wide variety of national security offenses, including economic espionage. 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

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.

stealing intellectual property through cyber-enabled means and proposes a strategy specifically designed to disrupt such efforts.

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.⁵ 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 (USTR) Special 301 process of evaluating the adequacy of our trading partners’ criminal IP laws and enforcement regimes; helping to catalogue and review the United States government’s IP training programs abroad; and implementing an aggressive international program to promote cooperative enforcement efforts with our trading partners and to improve substantive laws and enforcement regimes in other countries.

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

The Department achieved notable success in FY 2021 both domestically and abroad. Some of these efforts are highlighted below:

⁵ 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, Homeland Security Investigations (“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.

Prosecution Initiatives

The Department continues to prioritize IP-related 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 2021, this initiative resulted in a number of significant prosecutions, including those set forth below:

- *Georgia Couple Sentenced for Importing and Distributing Male Enhancement Products and Counterfeit Goods from China.* On February 24, 2021, Irfanali Momin and Shiba I. Momin a/k/a Saguftabanu Momin, husband and wife, both of Dahlonga, Georgia, were sentenced to prison for naturalization fraud and conspiring to illegally import and distribute misbranded drug products from China and traffic counterfeit goods, after pleading guilty in September 2020. These products contained sildenafil, the active pharmaceutical ingredient in Viagra, and/or tadalafil, the active pharmaceutical ingredient in Cialis. 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.
- *Ukrainian Traffickers Sentenced for Counterfeit Cancer and Hepatitis Drugs.* On March 25, 2021, Maksym Nienadov, 36, and Volodymyr Nikolaienko, 34, of Ukraine were sentenced to respective terms of 71 and 33 months in prison after admitting they conspired to smuggle and distribute counterfeit cancer and hepatitis drugs into the United States. Nienadov is the owner of the Ukrainian-based company Healthy Nation. He and Nikolaienko, his employee and co-conspirator, pleaded guilty to conspiracy, trafficking in counterfeit drugs and smuggling goods into the United States July 17, 2020.
- *Manufacturer Sentenced for Conspiring to Manufacture and Sell Counterfeit Goods.* On April 12, 2021, Bernard Klein, 40, a New York, New York, businessman, was sentenced to 18 months in federal prison and ordered to pay a \$15,000 fine. Klein pleaded guilty in August 2020 in District Court 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. Some of the counterfeit items were distributed to members of the United States military, including parkas 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.

- *Lebanon County Man Sentenced to Seventy Months' Imprisonment for Trafficking Counterfeit Drugs.* On April 15, 2021, Stefan Knoche, 55, of Lebanon, Pennsylvania, was sentenced to 70 months in prison for trafficking in counterfeit drugs, as well as ordered to pay \$3,648,911.18 in restitution. Knoche was charged in August 2020 by Criminal Information, which alleged that Knoche intentionally trafficked drugs knowing them to contain counterfeit marks of pharmaceutical manufacturers Pfizer Pharmaceuticals, Bayer AG, Eli Lilly and Company, and Roche Holding AG between May 23, 2017 and April 12, 2018. The information alleges Knoche knowingly trafficked counterfeit Viagra, Aurogra, Xanax, Levitra, Cialis, and Valium, all using counterfeit trademarks of their respective pharmaceutical companies.
- *Florida Man Sentenced for Selling Counterfeit Drugs on the Dark Net.* On August 24, 2021, Benjamin Burdick, 55, of Inverness, Florida, was sentenced to three years in prison for selling hundreds of thousands of counterfeit prescription drug pills through the Internet. According to court documents, from at least April 2019 until October 2020, Burdick sold at least 249,700 counterfeit Xanax pills through online hidden marketplaces. From his residence in Florida, Burdick used a pill press to manufacture pills that he stamped with the letters 'Xanax.' The pills that Burdick created did not contain just alprazolam, which genuine Xanax contains, but also contained substances such as flualprazolam, etizolam, adinazolam, and microcrystalline cellulose.

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

In FY 2021, 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:

- *Taiwan Company Pleads Guilty to Trade Secret Theft in Criminal Case Involving PRC State-Owned Company.* On October 28, 2020, United Microelectronics Corporation, Inc. (UMC), a Taiwan semiconductor foundry, pleaded guilty to criminal trade secret theft and was sentenced to pay a \$60 million fine, in exchange for its agreement to cooperate with the government in the investigation and prosecution of its co-defendant, a Chinese state-owned-enterprise. A federal grand jury indicted UMC in September 2018, along with Fujian Jinhua Integrated Circuit Co., Ltd. (Fujian Jinhua), a state-owned enterprise of the People's Republic of China (PRC), and three individuals for conspiracy to steal, convey, and possess stolen trade secrets of an American semiconductor company (Micron Technology, Inc. (Micron)) for the benefit of a state-owned enterprise of the PRC (Fujian Jinhua). As a result of the guilty plea, and in accordance with an accompanying plea agreement, UMC, whose American Depository Receipts are publicly traded on the New York Stock Exchange, will pay the fine—the second largest ever in a criminal trade

secret prosecution, be subject to a three-year term of probation, and cooperate with the United States.

- *Hospital Researchers Sentenced to Prison for Conspiring to Steal Trade Secrets and Sell Them in China.* On April 19, 2021, Yu Zhou, 51, of Dublin, Ohio, was sentenced to 33 months in prison for conspiring to steal exosome-related trade secrets concerning the research, identification, and treatment of a range of pediatric medical conditions. Zhou pleaded guilty in December 2020 to stealing scientific trade secrets related to exosomes and exosome isolation from Nationwide Children's Hospital's Research Institute for his own personal financial gain. Zhou also conspired to commit wire fraud. According to court documents, Zhou and his co-conspirator and wife, Li Chen, 48, worked in separate medical research labs at the Research Institute for 10 years each (Zhou from 2007 until 2017 and Chen from 2008 until 2018). They pleaded guilty to conspiring to steal at least five trade secrets related to exosome research from Nationwide Children's Hospital. Chen was sentenced in February to 30 months in prison for her role in the scheme.
- *Ph.D. Chemist Convicted of Conspiracy to Steal Trade Secrets, Economic Espionage, Theft of Trade Secrets and Wire Fraud.* On April 22, 2021, following a twelve-day jury trial, Dr. Xiaorong You, aka Shannon You, 59, of Lansing, Michigan, was convicted of conspiracy to commit trade secret theft, conspiracy to commit economic espionage, possession of stolen trade secrets, economic espionage, and wire fraud. You and Liu Xiangchen, 61, of Shandong Province, China, were originally indicted in February 2019 for trade secret offenses and wire fraud, and You was charged in a superseding indictment with economic espionage and conspiracy to commit economic espionage in August 2020, 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. In May 2022, You was sentenced to 168 months in prison along with a \$200,000 fine.
- *Niskayuna Man Sentenced for Stealing General Electric's Trade Secrets.* On April 30, 2021, Yang Sui, age 43, of Niskayuna, New York, was sentenced to one year of probation, and to pay a \$5,000 fine, for stealing trade secrets from General Electric Company (GE). As part of a May 2020 guilty plea, Sui admitted that between about January 1, 2015 and December 21, 2017, he stole multiple electronic files that contained GE's trade secrets related to the research, development, design and manufacture of its silicon carbide metal-oxide semiconductor field-effect transistors (MOSFETs), which are used in a variety of GE's parts and products, including aviation equipment and wind turbines.
- *Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research.* On May 28, 2021, four nationals and residents of the PRC were charged with a campaign to hack into the computer systems of dozens of victim companies, universities and government entities in the United States and

abroad between 2011 and 2018. The indictment, which was unsealed on July 16, 2021, alleges that much of the conspiracy's theft was focused on information that was of significant economic benefit to China's companies and commercial sectors, including information that would allow the circumvention of lengthy and resource-intensive research and development processes. The defendants and their Hainan State Security Department conspirators sought to obfuscate the PRC government's role in such theft by establishing a front company, Hainan Xiandun Technology Development Co., Ltd. (Hainan Xiandun), since disbanded, to operate out of Haikou, Hainan Province.

- *Former CEO And COO Of JHL Biotech Convicted Of Conspiracy To Steal Trade Secrets And Commit Wire Fraud Exceeding \$101 Million.* On August 24, 2021, Racho Jordanov, the co-founder and former Chief Executive Officer of JHL Biotech, and Rose Lin, another of the company's co-founders and former Chief Operating Officer, each were convicted of conspiracy to commit trade secret theft and wire fraud. According to the plea agreements, in 2012, Jordanov, 73, of Rancho Santa Fe, California, and Lin, 72, of South San Francisco, California, co-founded JHL Biotech, Inc., a biopharmaceutical startup in Taiwan. Between 2011 and 2019, Jordanov, as President and CEO of JHL Biotech, obtained and possessed confidential, proprietary, and trade secret information from Genentech, and used it to accelerate the timeline for and to reduce the costs of JHL Biotech's development and production of Genentech biosimilars and to enhance JHL Biotech's ability to meet various regulatory requirements related to the same. By various means, Jordanov obtained for JHL Biotech's use many confidential and proprietary documents from Genentech without authorization, some of which contained trade secret information. In so doing, he worked with multiple people within JHL Biotech, including Lin, to possess and use confidential, proprietary, and trade secret information he knew JHL Biotech was not authorized to have. In March 2022, Jordanov and Lin were each sentenced to a term of imprisonment of 12 months and one day, to be followed by a term of supervised release of 36 months.
- *Engineer Ends Trial by Pleading Guilty to the Federal Crime of Conspiring to Steal Trade Secrets.* On September 29, 2021, Gilbert Basaldua, 62, of Hilton Head, South Carolina, pleaded guilty to conspiring to steal trade secrets from aircraft companies and interstate transportation of stolen property during the second day of his jury trial. As alleged in the superseding indictment in the case filed in August 2020, Basaldua worked as a numerical control engineer contractor for an aircraft manufacturer from October 2016 through November 2018. During that time, Basaldua conspired with his co-conspirators to steal valuable proprietary aircraft wing designs and anti-icing testing information from various aircraft manufacturers, including the company where Basaldua worked.

(3) Large-Scale Commercial Counterfeiting and Online Piracy

The Department continues to pursue significant, large-scale piracy and counterfeiting operations. In FY 2021, the Department has had a number of significant prosecutions, including those set forth below:

- Three Members of Notorious Videogame Piracy Group “Team Xecuter” Charged.* On October 2, 2020, Max Louarn, 48, a French national, Yuanning Chen, 35, a Chinese national, and Gary Bowser, 51, a Canadian national, were charged with 11 felony counts, including conspiracy to commit wire fraud, wire fraud, conspiracy to circumvent technological measures and to traffic in circumvention devices, trafficking in circumvention devices, and conspiracy to commit money laundering. The indictment alleges the defendants were leaders of a criminal enterprise that developed and sold illegal devices that hacked popular videogame consoles so they could be used to play unauthorized, or pirated, copies of videogames. In September 2020, Bowser was arrested and deported from the Dominican Republic, and appeared on October 2, 2020, in federal court. Bowser pleaded guilty to two counts on October 28, 2021, in February 2022, he was sentenced to 40 months imprisonment and ordered to pay \$4.5 million in restitution. The United States is coordinating with French authorities on the potential arrest and extradition of Louarn to the United States.
- Former State Department Employee Sentenced to Prison for Trafficking in Counterfeit Goods from U.S. Embassy.* On March 18, 2021, former U.S. Department of State employee Gene Leroy Thompson, Jr., 54, and his spouse, Guojiao “Becky” Zhang, 40, were sentenced for their roles in a conspiracy to traffic hundreds of thousands of dollars in counterfeit goods through e-commerce accounts operated from State Department computers at the U.S. Embassy in Seoul, Republic of Korea. On December 20, 2020, Thompson Jr. and Zhang each entered guilty pleas to one count of conspiracy to traffic 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.
- Newport Man Sentenced to Federal Prison for Creating Illegal Video Streaming and Downloading Websites.* On July 9, 2021, Talon White, 31, of Newport, Oregon, was sentenced to 12 months and one day in federal prison and three years’ supervised release. White pleaded guilty on November 25, 2019 to one count each of criminal infringement of copyright 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 websites created by White and were able to stream or download the video content, including movies not yet released to the public. In total, White’s scheme netted more than \$8 million.
- Four New York Defendants Arrested in Multimillion-Dollar Counterfeit Goods Trafficking Scheme.* On August 11, 2021, a 14-count indictment was unsealed charging seven defendants with participating in an international scheme to traffic counterfeit goods between October 2019 and July 2021, in which they imported generic goods into the United States from China, applied brand labels to those goods in workshops, some of which were controlled by the defendants, and then sold those counterfeit-branded goods to retail and wholesale purchasers. The charges against the defendants include conspiracy

to traffic and trafficking in counterfeit goods and money laundering. Seven defendants—Hai Long Zhou, Saiyin Hou, Yan Xue Huang, Jian Fen Yang, Pi Zhong Zhou, Jian Fen Yang, and Xiao Bao Zhang—were arraigned and each was released on a \$200,000 bond. The estimated retail value of the counterfeit-branded goods, had they been genuine, was in excess of \$130 million.

- *Manhattan U.S. Attorney Announces Extradition Of British National For Participation In Online Film And TV Piracy Group.* On August 31, 2021, George Bridi, a citizen of the United Kingdom, was extradited to the United States from Cyprus. Bridi was arrested on August 23, 2020, in Paphos, Cyprus, and was extradited on charges of conspiracy to commit copyright infringement, wire fraud conspiracy, and conspiracy to commit interstate transportation of stolen property, for his involvement in the Sparks Group, an international piracy group that illegally distributed movies and television shows on the Internet. Previously, on August 26, 2020, the indictments were unsealed charging Umar Ahmad, 39, George Bridi, 50, and Jonatan Correa, 36, with copyright infringement. The Sparks Group has caused tens of millions of dollars in losses to film production studios. Co-defendant Jonatan Correa, a/k/a “Raid,” pleaded guilty to conspiracy to commit copyright infringement and was sentenced on May 19, 2021, to three years and three months of supervised release, with the first three months to be served in community confinement. Co-defendant Umar Ahmad, a citizen of Norway, remains at large. Bridi pleaded guilty to one count on November 18, 2021, and in February 2022, he was sentenced to 22 months imprisonment and ordered to pay \$120,000 in restitution.
- *NJ, NY, CA Defendants Indicted for Nationwide Copyrighted IPTV Theft Scheme.* On September 22, 2021, Bill Omar Carrasquillo, 35, of Swedesboro, New Jersey; Jesse Gonzales, 42, of Pico Rivera, California; and Michael Barone, 36, of Richmond Hill, New York, were charged by indictment with crimes arising out of a wide-ranging and lucrative copyright infringement scheme. According to the indictment, from about March 2016 until at least November 2019, the defendants operated a large-scale internet protocol television (IPTV) theft scheme in which they fraudulently obtained cable television accounts and then resold copyrighted content to thousands of their own subscribers, who could then stream or playback content. The defendants also allegedly made fraudulent misrepresentations to banks and merchant processors in an effort to obtain merchant processing accounts. During the period of their scheme, the defendants earned more than \$30 million. Carrasquillo, in particular, allegedly converted a large portion of his profits into homes and dozens of vehicles, including high-end sports cars. In January 2022 and February 2022, Gonzales and Carrasquillo pleaded guilty to copyright infringement conspiracy and wire fraud charges. In February and March 2023, Carrasquillo, Gonzales, and Barone were sentenced to 66 months, 28 months, and 14 months imprisonment, respectively, ordered to pay restitution in the amount of \$16.4 million, \$1.03 million, and \$122,402, respectively, and ordered to forfeit \$30.2 million, \$1.03 million, and \$122,402, respectively.

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 June 2021, CCIPS provided virtual instruction on ransomware investigations, theft of trade secrets, working with China, and infrastructure takedowns at a NAC course focusing on combatting transnational crime with a nexus to Russia, China, and other similar countries.
- In June 2021, CCIPS participated in an online panel discussion with the FBI and U.S. Attorney's Office in San Francisco titled the "Introduction to IPR Investigations." The panel was hosted by FBI San Francisco as part of its weekly series. The audience included private sector representatives and some law enforcement. CCIPS also provided an overview of DOJ and CCIPS resources to combat IP crimes.
- In June 2021, CCIPS presented to an audience of 80 HSI and FBI agents about the statutory structure and law enforcement resources for investigating and prosecuting online copyright piracy cases, including the recently-enacted Protect Lawful Streaming Act. Other presenters included representatives of the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), and The Software Alliance (BSA).
- In July 2021, CCIPS participated in an online panel discussion with the FBI and U.S. Attorney's Office in San Francisco involving the case study of *United States v. Shan Shi* (D.D.C.). The panel was hosted by FBI San Francisco, and the audience included private sector representatives and some law enforcement. CCIPS and an FBI intelligence analyst provided an overview of the investigation and prosecution of a theft of trade secrets case that went to trial in 2019.
- In July 2021, CCIPS presented at a virtual training for AUSAs organized by the Department's COVID-19 Fraud Enforcement Task Force. The presentation, titled "Cyber-Related Fraud and Internet Service Providers," focused on obtaining voluntary and compelled assistance from technology companies to disrupt and investigate COVID-19 and other cyber-enabled fraudulent schemes. Other presenters included attorneys from the Criminal Division's Fraud and MLARS sections, the Civil Division's Commercial Litigation Branch, the National Unemployment Fraud Task Force, the Organized Crime Drug Enforcement Task Force, and the International Organized Crime Intelligence and Operations Center (IOC-2).
- In August 2021, CCIPS hosted the Computer Hacking and Intellectual Property (CHIP) Prosecutors' Conference virtually via WebEx. Attendees included prosecutors from U.S. Attorneys' Offices and Main Justice components who have been designated a CHIP for their office. This year, due to the increased attendance made possible by the conference taking place online, additional prosecutors who are not CHIPS—but nonetheless have an interest in

computer crime, electronic evidence, and/or intellectual property offenses—also attended. The conference provided attendees with the latest information and guidance with respect to the collection and use of electronic evidence, computer crime, intellectual property crime, and related issues. The conference was organized by the National CHIP Coordinator and CCIPS with the assistance of the CHIP Working Group.

- In September 2021, CCIPS provided a virtual training during a four-day course hosted by the IPR Center. The series consisted of trainings on intellectual property and trade enforcement investigations. CCIPS presented to a group of agents and attorneys regarding relevant statutes, including IP-related federal crimes, that agents may come across during their investigations.

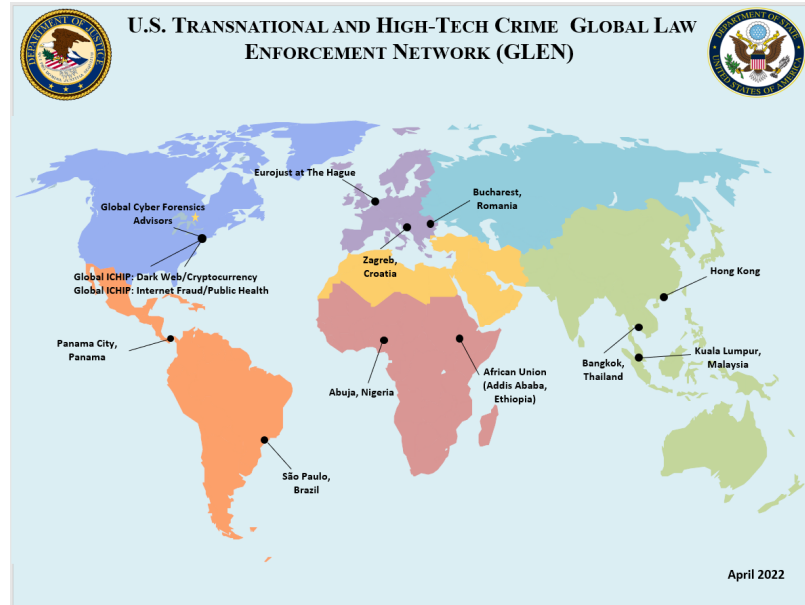
International Outreach and Training

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 2021, 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 2021, 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 2021, the Department, with assistance from the State Department, continued to support the recently expanded 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 ("IPLC") program). DOJ has 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 includes two ICHIPs based in the United States to serve as global subject matter experts in dark web and cryptocurrency issues ("DWC") and internet-based fraud and public health ("IFPH") issues. Additionally, the GLEN includes Global Cyber Forensic Advisors 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.⁶

⁶ For more information about CCIPS' international outreach, see <https://www.justice.gov/criminal-ccips/overseas-work>.



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

ASIA

Presented in Indo-Pacific IPR Enforcement Series: In October and November 2020, ICHIP Hong Kong and the IFPH ICHIP partnered with the United States Patent and Trademark Office (USPTO) and the Association of Southeast Nations (ASEAN) Secretariat to present webinars in their Indo-Pacific IPR enforcement series. Over one hundred prosecutors, customs officers, administrative enforcement officials, criminal investigators, and IP rights holders from more than fifteen ASEAN countries registered for the webinars.

Participated in the 2020 Global Cooperation and Training Framework (GCTF) Virtual Conference on Trade Secrets Protection and Digital Piracy Prevention. In October 2020, ICHIP Hong Kong and the DWC ICHIP participated in the 2020 GCTF Virtual Conference on Trade Secrets Protection and Digital Piracy Prevention, co-sponsored by the American Institute in Taiwan, the Taiwan Ministry of Justice and the Japan-Taiwan Exchange Association. Speakers from the U.S., Taiwan and Japan delivered a virtual presentation to participants from countries across Asia and the Pacific Islands.

IPR Enforcement Workshop for Vietnam’s Directorate of Market Surveillance. In October 2020, ICHIP Hong Kong organized its first hybrid live/virtual IPR enforcement workshop for Vietnam’s Directorate of Market Surveillance (DMS). Thirty DMS officials each gathered at conference venues in Hanoi and Ho Chi Minh City.

Presentation entitled: “The Emerging Markets of Online Counterfeiting.” In November 2020, ICHIP Hong Kong and the IFPH ICHIP teamed with Philippines Intellectual Property Office

(IPOP/HIL) Head to deliver a presentation, entitled “The Emerging Markets of Online Counterfeiting,” for AmCham Philippines.

Panelist for “Scams, Frauds and Misdeeds on the Internet” at the 2020 Annual Meeting of the International Trademark Association. In November 2020, ICHIP Hong Kong participated in a panel on “Scams, Frauds and Misdeeds on the Internet” at the 2020 Annual Meeting of the International Trademark Association (INTA), which was held virtually this year. The panel focused on the latest and greatest internet fraud schemes, with special attention devoted to those involving the use of counterfeit trademarks and those leveraging current events, such as the COVID-19 pandemic and the Black Lives Matter movement.

Participated in the Third Country Training Programme Workshop: “Adapting IP Laws to Promote Innovation and Creativity in New Technologies.” In January 2021, ICHIP Hong Kong participated in the 2020-21 virtual Third Country Training Programme (TCTP) workshop “Adapting IP Laws to Promote Innovation and Creativity in New Technologies,” principally organized by USPTO. ICHIP Hong Kong sat on a panel entitled “Challenges and Strategies for Enforcement in an Online and Transnational Environment.” TCTP is a joint initiative of the U.S. government and the government of Singapore to provide training for the other ASEAN member states.

Participated in the Third Berkeley-Tsinghua Conference on Transnational IP Litigation. In January 2021, ICHIP Hong Kong participated in the Third Berkeley-Tsinghua Conference on Transnational IP Litigation, attended virtually by approximately 400 people in the U.S. and China. ICHIP Hong Kong appeared on a panel on “Trade Secrets Law and Litigation.”

Organized Virtual Workshop on “Investigation of Online IPR Crimes.” In April 2021, in Manila, Philippines, ICHIP Hong Kong organized a virtual workshop on “Investigation of Online IPR Crimes,” principally for the Philippines Optical Media Board (OMB), but open to other civil enforcement agencies in the country. The Economic Section at U.S. Embassy Manila co-sponsored the virtual program. Over 150 officials from OMB and other civil enforcement agencies in the Philippines attended. The workshop included presentations from CCIPS on attribution, IFPH ICHIP on best practices for investigating online crimes, and ICHIP Kuala Lumpur on best practices for obtaining electronic evidence from third parties.

Organized IPR Enforcement Workshop. In April 2021, in Halong Bay City, Vietnam, ICHIP Hong Kong staged a hybrid live/virtual IPR enforcement workshop for Vietnam’s MPS and provincial police units. The U.S. Department of State Bureau of International Narcotics and Law Enforcement Affairs Hanoi regional office (INL Vietnam) and the U.S. Embassy Hanoi Economic Section (ECON) co-sponsored the workshop. Forty-one MPS and provincial police officers attended, including several from newly formed cybercrime units. Speakers included, among others, the IFPH ICHIP who presented virtually on best practices for investigating online crimes, ICHIP Kuala Lumpur who presented on obtaining electronic evidence from third parties, a CCIPS attorney who presented on attribution, and industry representatives who addressed the private sector’s view on combating digital piracy.

NORTH AFRICA AND THE MIDDLE EAST

Participant at the Commercial Law Development Program's Central Asia Regional Expert Level Working Group. In January 2021, ICHIP Bucharest joined the Commercial Law Development Program's (CLDP) Central Asia Regional Expert Level Working Group on Intellectual Property to discuss IP issues with representatives from Kazakhstan, Kyrgyz Republic, Tajikistan, Turkmenistan, and Uzbekistan. This interagency coordination meeting involved representatives from CLDP, the Office of the USTR, the IPR Center, and CBP.

CENTRAL AND SOUTH AMERICA

Webinar on IPR Enforcement Issues and COVID-19 Organized by the International Trademark Association. In October 2020, ICHIP São Paulo shared tips for reporting online COVID-19 scams to U.S. service providers, particularly domain registrars, to approximately 140 law enforcement officials and brand protection representatives drawn from around Central America at webinar on IPR enforcement issues and COVID-19 organized by the International Trademark Association (INTA).

Speaker at Program Organized by the Mexican Intellectual Property Institute for Participants from the Mexican Legal and Regulatory Community. In December 2020, ICHIP Panama spoke at a virtual program organized by the Mexican Intellectual Property Institute (IMPI) about trending issues in copyright enforcement online content to approximately 100 participants from the Mexican legal and regulatory community.

Presentation on Trade Secrets Theft and Economic Espionage to a Group of Appellate Judges in the Mexican Institute of Industrial Property. In February 2021, ICHIP São Paulo presented on the topics of trade secrets theft, economic espionage, and electronic evidence gathering to a group of appellate judges in the Mexican Institute of Industrial Property. The program was arranged by the USPTO in Mexico City and the program provided an overview of the Economic Espionage Act and the manner in which US prosecutors enforce trade secret laws while protecting victims.

Presentation to 20 Uruguayan Officials and Rights Holders to Introduce the ICHIP Program and Provide an Overview of IP Crime. In March 2021, ICHIP São Paulo delivered a virtual presentation introducing the ICHIP program and providing an overview of IP crime to a group of more than 20 Uruguayan officials and rights holders.

Presented to Senior Dominican Republic Officials on Inter-agency Communication and Best Practices to Combat Intellectual Property Theft. In March 2021, ICHIP São Paulo, in conjunction with U.S. Embassy Santo Domingo, USPTO and HSI, presented on the topic of inter-agency communication and best practices to combat Intellectual Property theft to a group of senior Dominican Republic (DR) officials, including the Deputy Attorney General and leaders of the Patent, Copyright, and Health ministries. The presentation demonstrated how to address IP

theft using a whole-of-government approach and highlighted opportunities, through the ICHIP program, for the DR to have an ongoing dialogue with regional partners on best practices.

Discussion on Trends in COVID-19 Fraud for Ecuadorean Prosecutors and Public Health Officials. In April 2021, ICHIP São Paulo led a discussion about current trends in COVID-19 Fraud for a group of approximately 140 Ecuadorean Prosecutors and Public Health officials. The ICHIP noted that the threat landscape associated with COVID-19 vaccines is constantly evolving and discussed methods by which the Ecuadorean authorities can quickly detect and share useful intelligence throughout their nation.

Hosted Industry Panel on COVID-19 Related Frauds for Brazilian Customs, Health Ministries and Federal Prosecutors' Offices. In April 2021, ICHIP São Paulo and ICHIP IFPH, along with an HSI Attaché, hosted a virtual industry panel on COVID-19 related frauds for approximately 200 Brazilian customs, health ministries, and federal prosecutors' offices covering 23 of 26 Brazilian states and the capital federal district. The panel, which included security officials from three major vaccine manufacturers, discussed the current threat landscape regarding counterfeit vaccines and frauds associated with the pandemic both in Latin America and throughout the world.

Hosted Virtual Industry Panels on COVID-19 Related Frauds for Law Enforcement Representatives from Across the Caribbean and Central and South America. In April and May 2021, ICHIPs São Paulo and IFPH hosted virtual industry panels on COVID-19 related frauds for approximately 190 prosecutors, police, customs, and health ministry officials from Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Peru, Suriname, and Trinidad and Tobago. During the panels, industry representatives discussed the current threat landscape regarding counterfeit vaccines and frauds associated with the pandemic both in Latin America and throughout the world.

Series of Presentations on Whole of Government Approach to Combatting IP Crimes in Goiânia, Goiás. In June 2021, the ICHIP São Paulo, ICHIP Special Agent, and ICHIP Staff Attorney gave a series of presentations to approximately 65 federal, state, highway, and military police; customs officials; and health and environmental ministry officials on the importance of using a whole-of-government approach to combatting IP crimes, including counterfeit agricultural chemicals in Goiânia, Goiás.

Presented at the IP Rights Conference in Punta Cana, Dominican Republic. In August 2021, ICHIP São Paulo and CCIPS shared their expertise with 85 prosecutors and police officers from 14 Caribbean countries at an HSI-organized IP rights conference in Punta Cana, Dominican Republic. The ICHIP and CCIPS focused on DOJ's response to IP offenses and tactics to identify, preserve, and obtain evidence from the United States.

Held Series of Workshops to Encourage Brazilian Police and Prosecutors to Collaborate and Coordinate During Significant IPR Case Investigations. In August, September, and October 2021, ICHIP São Paulo and ICHIP IFPH held a series of workshops designed to encourage Brazilian police and prosecutors to collaborate and coordinate their actions earlier in the investigative process during significant IPR cases. The presentations featured a team of federal

prosecutors and agents that worked together to investigate and prosecute IP and cyber cases as a coherent team.

EUROPE

Panel on “The Role of Intellectual Property and the Need for Better Protection” at Aspen Institute’s Bucharest Forum. In October 2020, ICHIP Bucharest organized and moderated a panel at the Aspen Institute’s Bucharest Forum on the role of intellectual property and the need for better protection. The Bucharest Forum, initiated in 2012, is a high-level regional event involving government officials, industry leaders, and civil society designed to address and foster innovative thinking on the greatest challenges Europe is facing.

Webinar with Romanian Association for Information Security Assurance titled: “Methods for Fighting Intellectual Property Crime and Online Forgery.” In December 2020, ICHIP Bucharest partnered with the Romanian Association for Information Security Assurance (RAISA) for their webinar “Methods for Fighting Intellectual Property Crime and Online Forgery” where he presented an overview of the counterfeit pharmaceutical problem, with a particular emphasis on the counterfeiting of drugs that has arisen during the COVID-19 pandemic. The event was attended by more than 100 Romanian judges, prosecutors, police officers, and students from the Romanian Police Academy.

Online Seminar with the Latvian School of Public Administration on Preventing and Combatting Counterfeiting and Fraud in the Pharmaceutical and PPE Industries. In January 2021, ICHIP Bucharest and RLA for the Baltics, based in Latvia, co-hosted an online seminar with the Latvian School of Public Administration on preventing and combatting counterfeiting and fraud in the pharmaceutical and personal protective equipment industries. The program featured experts from the U.S. Attorney’s Office of the District of North Dakota, Latvian State Police, Latvian Prosecutor General’s Office, World Health Organization, Interpol, European Directorate for the Quality of Medicines & Healthcare, Italian Medicines Agency, Italian Carabinieri, as well as representatives from Merck and Pfizer.

Webinar for Bulgarian National Customs Agency Officials on Fighting Counterfeit Pharmaceuticals and COVID-19 related Crimes. In May 2021, OPDAT RLA for Bulgaria and Romania and ICHIP IFPH hosted a webinar to discuss ways of fighting counterfeit pharmaceuticals and COVID-19 related crimes with 23 officials of the Bulgarian National Customs Agency.

SUB-SAHARAN AFRICA

Webinar Series for the Anglophone Pharmacrime Working Group. In September, October, and November 2020, ICHIP Abuja and ICHIP IFPH hosted a series of webinars, entitled “Fighting Fraud and Fake Meds in the Time of COVID-19,” for the Anglophone Pharmacrime Working Group (AWG). HSI spoke to the group about developing customs seizures into criminal investigations and prosecutions, describing such investigative techniques as controlled deliveries, undercover purchases, and working closely with brand owners. Working group members from Kenya, Nigeria, Uganda, Ghana, the Gambia, Liberia, Namibia, and South Africa discussed

which techniques may be available in their countries as well as issues they may encounter, including price gouging and offering fictitious products for sale via text messages.

Pharma Crime Working Group Webinar in Accra, Ghana. In October 2020, ICHIP Abuja and ICHIP IFPH conducted an Anglophone pharma crime working group webinar, hosted by the RTC in Accra, Ghana. The Working Group member from Namibia discussed a case study involving a customs seizure that developed into a criminal case.

Workshop for Nigerian Judicial Officers on “Fraudulent Medicines and Intellectual Property Crimes in the Digital Economy: A Judicial Officer’s Approach.” In October 2020, ICHIP Abuja organized and led an Intellectual Property Rights Enforcement Virtual Workshop for Nigerian Judicial Officers on fraudulent medicines and other IP crimes in the digital economy.

Panel Member in Virtual Anti-Counterfeit and Illicit Trade Initiative Hosted by the American Business Council. In October 2020, ICHIP Abuja participated as a panel member in a virtual Anti-Counterfeit and Illicit trade initiative hosted by the American Business Council (ABC) in partnership with Pfizer Specialties Limited. The ICHIP spoke on capacity-building initiatives aimed at training staff of agencies on combatting illicit pharma criminal offenses.

Webinar with 20 Anglophone Pharmacrine Working Group Members About Tactics for Fighting Pharmaceutical Crimes. In December 2020, ICHIP Abuja and ICHIP IFPH co-led a discussion with 20 Anglophone Pharmacrine Working Group members (WGM) about tactics for fighting pharmaceutical crimes. The webinar began with a country presentation from the WGM from Zambia and focused on ways to fight drug diversions, including diversions of pharmaceuticals donated by U.S. NGOs, as observed by WGMs from both Zambia and South Africa. The meeting then evolved to a group discussion of how to address issues such as prevention, public awareness, and local police who tip off targets.

Webinar on IP Infringement, Innovation, and the Economy, Sponsored by the American Business Council. In December 2020, ICHIP Abuja was a panel member in a webinar on IP infringement, innovation, and the economy, sponsored by the American Business Council in Lagos. In this program, the ICHIP described U.S. efforts to build capacity among IP criminal law enforcement officials.

Hosted Virtual Meetings of the Joint Pharmacrine Working Group for 26 African Countries. From February through May 2021, ICHIP Abuja and ICHIP for Internet Fraud and Public Health (IFPH) hosted virtual meetings of the Joint Pharmacrine Working Group. These meetings combined prosecutors and investigators from ICHIP Abuja’s Anglophone and Francophone Working Groups. Working group members discussed techniques for following the money, identifying fraudulent websites, and international coordination.

Virtual World Intellectual Property Day Program, “IP and Small and Medium-sized Enterprises (SME): Taking Your Ideas to Market.” In April 2021, ICHIP Abuja participated in the virtual World Intellectual Property Day program, on which it had coordinated with the Nigeria Office of the World Intellectual Property Organization. The program’s theme was “Innovation, IP and SMEs: Opportunities and Challenges for SMEs in Driving Nigeria’s Economic Recovery.” This

high-level event included a keynote address from the Minister of Trade and Commerce, speaking on behalf of the Vice President of Nigeria and prerecorded remarks from the U.S. Ambassador.

Participated in IP Webinar, titled "Exploring How African Creative Artists Can Protect Their Work." In May 2021, ICHIP Addis Ababa participated in a three-hour Intellectual Property webinar, along with the U.S. Mission to the African Union, which drew over 117 viewers from three continents.

Hosted Training for the Nigerian Federal Agencies Network Against Counterfeiting and Piracy. In June 2021, ICHIP Abuja hosted a training program for the Nigerian Federal Agencies Network Against Counterfeiting and Piracy (FANCAP) in acknowledgement of World Anti-Counterfeiting Day. The Customs Service, the Copyright Commission, the National Agency for Food and Drugs Administration and Control, the Federal Competition and Consumer Protection Commission, and the Standards Organization participated.

Outreach to the Private Sector

The Department continues to reach out to the victims of IP crimes in a wide variety of ways, including during the operational stages of cases and through more formal training programs and conferences. For example, in FY 2021, CCIPS virtually held its Fourteenth Annual IP Industry and Law Enforcement Meeting in October 2020. 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. Senior law enforcement officials from DOJ, HSI, FBI, CBP, and FDA-OCI provided updates on their agencies' enforcement efforts and initiatives, approximately 200 industry and government 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 FY2021, the Criminal Division's high-level officials and CCIPS and ICHIP attorneys, as well as the Civil Division's Consumer Protection Branch attorneys, have also presented at a variety of domestic and international conferences, symposia, workshops, and events attended by IP rights holders and law enforcement officials. These events included, among others:

- In October 2020, CCIPS presented on criminal trademark infringement and trade secret theft for the U.S. Department of Commerce, International Trade Administration's virtual roadshows, STOPfakes.
- In October 2020, CCIPS and the IPR Center co-hosted a virtual meeting of the Counterfeit Microelectronics Working Group to discuss ways to detect and prevent distribution of counterfeit microelectronics in the U.S. supply chain. The meeting included speakers from Customs and Border Protection – Electronics Center of Excellence and Expertise, the Naval Surface Warfare Center, and Amazon's Counterfeit Crimes Unit, as well as a case study presented by the U.S. Attorney's Office for the Central District of California and NASA's Office of the Inspector General.

- In October 2020, ICHIP Hong Kong presented at a webinar organized by the USPTO China team on “How the U.S. Government Can Help Companies Protect and Enforce their IP in China,” attended by over 400 U.S. rights holders’ representatives. ICHIP Hong Kong joined representatives from the USPTO IP Attaché office in Guangzhou, China, the International Trade Administration IP office, the U.S. Department of State IP enforcement office, the U.S. Export Assistance Centers, U.S. Customs and Border Protection, the office of the USTR, and the U.S. Foreign & Commercial Service in Beijing.
- In October 2020, ICHIP Abuja spoke at a Regional IP Dialogue Series for Sub-Saharan Africa, sponsored by the International Anti-Counterfeiting Coalition. This webinar focused on Sub-Saharan Africa, centering on cross-border enforcement and highlighting the tools and “on-the-ground” assistance available to rightsholders in the region.
- In November 2020, CCIPS and ICHIP Abuja virtually presented on cyber-enabled IP crime at INTERPOL’s Ninth Regional Intellectual Property Crime Conference. The conference was attended by police, investigators, customs officers, and private sector representatives from the Middle East and North Africa Region.
- In December 2020, CCIPS joined representatives of USPTO, CBP and 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 200 participants representing brand owners, government officials, and members of the academic community.
- In December 2020, ICHIP Hong Kong in an International Anti-Counterfeiting Coalition webinar entitled “Dialogue with Amazon.” In addition to ICHIP Hong Kong, representatives from Amazon’s new HQ2 counterfeit crime unit presented at the webinar.
- April 2021, for World IP Day, ICHIP Hong Kong co-organized with the Consulate General Hong Kong Economic Section a roundtable for a broad group of rights holders and trade association representatives involved in IPR enforcement in Hong Kong.
- In June 2021, CCIPS met virtually with a six-attorney delegation from the IP Section of the California Lawyers Association. Topics of discussion included IP enforcement, cybersecurity issues, international engagement, legislative developments, and DOJ initiatives relating to both cybercrime and IP enforcement.

The Department maintains a website that, among other things, provides the public with information on the Department’s IP enforcement efforts, assists victims in understanding where and how to report an IP crime, and provides guidance on case referrals. That site can be found at <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 many 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.

(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 2021, listing the number of defendants and cases charged, the number of defendants sentenced, and the length of those sentences.⁷ Section 404(b) of the PRO IP Act 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.

⁷ 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 (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. § 2320 (trafficking in counterfeit goods); and 47 U.S.C. §§ 553 & 605 (signal piracy). The database does not contain data for 17 U.S.C. §§ 1202 to 1205 and 18 U.S.C. § 2319B. 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. This chart may not include cases or defendants if only a conspiracy to violate one of these offenses was charged.

District Totals	FY 2021
Investigative Matters Received by AUSAs	164
Defendants Charged	56
Cases Charged	34
Defendants Sentenced	41
No Prison Term	20
1-12 Months	5
13-24 Months	8
25-36 Months	3
37-60 Months	3
60 + Months	2

In addition, the chart below details FY 2021 statistics for criminal IP cases broken down by type of charge.⁸

Charge	Cases charged	Percentage
Trademark <i>Trafficking in counterfeit goods, 18 U.S.C. § 2320</i>	18	50%
Copyright <i>Criminal copyright infringement, 17 U.S.C. § 506; 18 U.S.C. § 2319</i>	5	14%
<i>Counterfeit labels, 18 U.S.C. § 2318</i>	0	0%
<i>DMCA, 17 U.S.C. § 1201</i>	1	3%
Economic Espionage Act <i>Economic espionage, 18 U.S.C. § 1831</i>	3	8%
<i>Theft of trade secrets, 18 U.S.C. § 1832</i>	9	25%
Total	36	100%

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

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

The Criminal Division currently devotes 17 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 25 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 the United States who have global subject matter expertise in dark web and cryptocurrency issues and internet-based fraud and public health issues, respectively. Global Cyber Forensic Advisors are 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 Global Cyber Forensic Advisors.

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, 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	<i>Digital Millennium Copyright Act</i>
DOJ	Department of Justice
EOUSA	Executive Office for United States Attorneys
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FY	Fiscal Year
HSI	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	<i>Prioritizing Resources and Organization for Intellectual Property Act of 2008</i>
USPTO	United States Patent and Trademark Office