



ANNUAL
INTELLECTUAL PROPERTY
REPORT TO CONGRESS

April 2022

“If we invest in ourselves and our people, if we fight to ensure that American businesses are positioned to compete and win on the global stage, if the rules of international trade aren’t stacked against us, if our workers and intellectual property are protected, then there’s no country on Earth — not China or any other country on Earth — that can match us.”

-- President Joe Biden¹

“We are proud to be a Nation of inventors and my Administration is committed to bolstering American industrial and innovative strength so we can continue to lead in making the cutting-edge products and services of tomorrow. My Administration is also committed to giving everyone, no matter where they are from, a chance to succeed and to contribute to creating the strongest, most resilient, innovative economy in the world.”

-- President Joe Biden²

¹ Remarks by President Biden on America’s Place in the World, February 04, 2021 available at: <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/>

² A Proclamation on World Intellectual Property Day, 2021, April 23, 2021, available at: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/04/23/a-proclamation-on-world-intellectual-property-day-2021/>

IPEC ANNUAL INTELLECTUAL PROPERTY REPORT TO CONGRESS:

This report is submitted pursuant to 15 U.S.C. §8114.

The Annual Intellectual Property Report to Congress, developed by the Office of the U.S. Intellectual Property Enforcement Coordinator, brings together the combined and coordinated efforts of the White House, the Departments of Agriculture, Commerce, Defense, Health and Human Services, Homeland Security, State, and Treasury, the Office of the U.S. Trade Representative, and the U.S. Copyright Office. What follows is an overview of the intellectual property enforcement strategy and related efforts undertaken by departments and agencies during fiscal year 2021.

APPENDICES

To the Annual Intellectual Property Report to Congress

1. Department of Agriculture	5
2. Department of Commerce.....	10
3. Department of Defense	42
4. Department of Health and Human Services	47
5. Department of Homeland Security	63
6. Department of Justice	85
7. Department of State	152
8. Department of Treasury	169
9. Office of the U.S. Trade Representative.....	172
10. Copyright Office	182

DEPARTMENT OF AGRICULTURE

DEPARTMENT OF AGRICULTURE

Department of Agriculture Appendix for FY 2021 Annual Report

This appendix discusses the FY 2021 activities of the Department of Agriculture.

Geographical Indications (GIs)

Overview

Article 22(1) of the Agreement on Trade-Related Aspects of Intellectual Property Rights provides that “[g]eographical indications are, for purposes of this Agreement, indications which identify a good as originating in the territory of a Member, or a region or locality in that territory, where a given quality, reputation or other characteristic of the good is essentially attributable to its geographical origin.”

USDA’s GI-related Activities during Fiscal Year (FY) 2021

The Foreign Agricultural Service (FAS) of the Department of Agriculture actively works with other Federal agencies, particularly the lead agencies USTR and USPTO, to monitor and directly engage with countries on the issue of geographical indications (GIs). USDA’s main goal is to ensure GI protections do not disadvantage U.S. producers by unfairly granting protection to products with common names and generic terms, which could ultimately result in a loss of market access.

During FY 2021, USDA engaged at the most senior levels with key foreign country counterparts to underscore concerns and counter harmful GI policies, emphasizing the importance of transparency, adherence to internationally recognized standards, an opportunity to comment on any proposed GIs through a comment period, and fair evaluations. USDA worked with interagency partners to engage a number of countries to raise the importance of procedural fairness and transparency as well as preserving common terms for food products; the countries included Chile, the MERCOSUR countries, Saudi Arabia, China, the European Union (EU), Kenya, and Korea.

Consortium for Common Food Names Activities Supported by USDA

The information below represents notable actions taken by the Consortium for Common Food Names (CCFN) in FY 2021. The U.S. Dairy Export Council, on behalf of a number U.S. agricultural associations including the U.S. Meat Export Federation and California Wine Institute, established CCFN in 2013 to monitor and combat GI-related trade restrictions. These activities are partially supported by USDA’s Market Access Program through a Global Broad-based Initiative. Since 2013, CCFN has received \$200,000 in funding annually from USDA for these efforts. Each item listed helped preserve U.S. exporters’ rights to use common food names.

- CCFN coordinated responses to various ongoing EU FTA negotiations, including:
 - Australia – EU FTA: Attended and participated in the virtual stakeholder briefing event that was held on March 30, 2021. Questions were submitted to the officials hosting this event to pursue confirmation that Australia will abide by its prior international commitments with respect to GIs and generic usage.
 - Chile – EU FTA: CCFN participated on May 2021 in the stakeholder meeting organized by the Under-Secretariat of International Economic Relations of the Chilean government, to inform the public about the status of GI negotiations in the ongoing EU-Chile FTA. CCFN submitted questions concerning the opposition and cancellation procedures that will be available under the Agreement, as well as provisions or guidelines regarding generic terms.
 - Vietnam – EU FTA: CCFN submitted a letter to Vietnam’s National Office of Intellectual Property, copying the Ministry of Industry and Trade and the Ministry of Science and Technology, to urge further clarity and action on how Vietnam is implementing certain provisions of the EU-Vietnam FTA that pertain to grandfathered generic users.

- CCFN continued outreach with international organizations, raising the profile of common food names with the World Intellectual Property Organization (WIPO) as a new Director General and his team assumed leadership. CCFN’s communications outlined the steps WIPO could take to provide greater balance on the issue of GIs in its programming and resulted in half of the speakers at their September 2021 Worldwide Symposium on Geographical Indications addressing generic users’ issues. CCFN participation focused on the impacts – on both local industries and trading partners – that result from GI restrictions on the use of generic terms. Comments also highlighted the need for stronger protections for common names around the world and cited the lack of consistent policies and due process protections that limit generic users’ rights. The panel was watched by approximately 300 participants.

- CCFN participated and collaborated on educational activities to raise awareness in foreign markets about the potential trade barriers that GIs may pose to local industries and trading partners. CCFN participated in the WIPO Working Group on the Development of the Lisbon System in November 2020, alongside 72 participants from various countries and industries. CCFN also presented on *Geographical Indications, How to Achieve the Right Balance in their International Protection* at the World Intellectual Property Forum in April 2021. This conference was attended by more than 1,500 people from over 30 countries. In addition, CCFN was a panelist at the June 2021 African Regional Intellectual Property Organization (ARIPO) GI Workshop, a webinar to educate intellectual property officials in Africa about GI issues and the importance of ensuring that producers relying on generic terms retain the ability to use them; about 60 participants from the ARIPO 19-country region participated in the event.

- CCFN submitted comments to Australia, Mexico, and the EU on GI regulations, outlining recommendations on how to best preserve the rights of common name users. CCFN also successfully opposed the recognition of GIs threatening the use of key generic terms. For example, the EU IP Office ruled in October 2020 against a Swiss appeal seeking to register the generic term “Emmental” as a trademark. Evidence provided by CCFN helped to support the EU IP Office’s determination that it remains a generic term. CCFN’s opposition to a trademark application in Turkey for “Mozzarella” resulted in the Office agreeing to remove dairy from the scope of goods covered by the trademark in June 2021. In addition, CCFN opposed a trademark application submitted by the Consortium for the Protection of the Gorgonzola Cheese for the United Arab Emirates, which resulted in the local IP Office denying the registration in June 2021.
- CCFN developed a trademark logo that can be registered globally to preserve common usage rights with a disclaimer for generic terms. Rights to use the trademark will be extended to generic name users to establish strong protections against bad-faith GI applications. Through FY Q4 2021, the following Madrid Protocol applications were granted: “CCFN Asiago,” “CCFN Bologna,” and “CCFN Feta” in Australia and “CCFN Provolone” in China. Directly-filed national trademarks applications were approved for “CCFN Asiago,” “CCFN Feta,” and “CCFN Parmesan” in Chile; “CCFN Feta” in Costa Rica; and “CCFN Asiago” and “CCFN Parmesan” in Brazil.

Plant Variety Protection

USDA plant variety protection certificates are recognized worldwide and expedite foreign plant variety protection application filing. The USDA Agricultural Marketing Service (AMS)’s Plant Variety Protection Office (PVPO) works actively with members of the International Union for the Protection of New Varieties of Plants (UPOV) to promote cooperation on the standards for variety examination. Once plant variety protection is granted, the certificate owners have exclusive legal rights to market and to exclude others from selling their varieties. This legal protection for breeders and inventors promotes the development of new varieties that can increase yield and crop productivity, increase farmer income, and expand trade opportunities. Other benefits of plant variety protection include provisional protection upon application receipt, priority when filing in another country, user-friendly filing without the need for an attorney, no annual maintenance fees, and applicant-conducted field trials. FAS encourages free trade agreement partners to become UPOV members to protect U.S. plant breeders’ rights across the globe.

USDA Plant Variety Protection Activities in FY 2021

PVPO received 500 applications for sexually reproduced, tuber propagated, and asexually reproduced varieties during the fiscal year. Among these were more than 20 applications for asexually reproduced varieties including varieties of almond, anthurium, apple, camellia, hemp, magnolia, mandarin, orchid, phlox, and strawberry.

PVPO staff provided four webinars – on the program, the electronic Plant Variety Protection System, and examination procedures – to participants from the European Union Community

Plant Variety Office, The International Community of Breeders of Asexually Reproduced Horticultural Plants (CIOPORA), American Seed Trade Association (ASTA), and Seed Innovation and Protection Alliance. The webinars highlighted the benefits of the electronic system, an overview of PVPO examination procedures, and how the addition of asexually reproduced varieties has been implemented. PVPO actively works with ASTA, CIOPORA, and other seed and vegetative industry stakeholders regularly.

New members were appointed to the Plant Variety Protection (PVP) Board on September 30, 2020. The Board consists of 14 members representing farmers, the seed industry, trade and professional associations, and public and private institutions involved with developing new plant varieties. Members of the PVP Board provide oversight and guidance to the program on plant variety protection issues.

AMS provides intellectual property rights protection through PVPO, which protects breeders of varieties of seed and tuber (potatoes) propagated plants, and asexually reproduced plants that are new, distinct, uniform, and stable. Authorized by the Plant Variety Protection Act, PVPO examines new variety characteristics to grant certificates that protect varieties for 20 years (25 years for vines and trees).

Agricultural Research Service's Protection of USDA's Own Intellectual Property

USDA's Agricultural Research Service (ARS) has a comprehensive program to protect U.S. Government-owned intellectual property. In addition to IP protection, ARS delivers a comprehensive training program on IP. The program has four components: (1) training scientists on Dual Use Research of Concern, Technology Transfer (TT), and insiders' threats; (2) training TT Staff on U.S. Department of Commerce regulations; (3) Export Control Reviews; and (4) entrance and exit procedures for agency employees to minimize insider threats.

DEPARTMENT OF COMMERCE

DEPARTMENT OF COMMERCE

Department of Commerce Appendix for FY 2021 Annual Report

This appendix discusses the FY 2021 activities of the Commerce Department, through the Commercial Law Development Program (CLDP), the International Trade Administration (ITA), the National Telecommunications and Information Administration (NTIA), and the U.S. Patent and Trademark Office (USPTO). The Commerce Department continues to engage in training and capacity building programs to strengthen intellectual property awareness and enforcement internationally. Additionally, the USPTO provides many different patent, trademark, copyright, and trade secret capacity building programs as fully described in our TRIPS Article 67 report each year, and the following highlights some enforcement activities during FY 2021.

COMMERCIAL LAW DEVELOPMENT PROGRAM

The Commerce Department's Commercial Law Development Program (CLDP) creates a level playing field for U.S. firms overseas, in particular by building the capacity of foreign countries to improve the protection and enforcement of intellectual property rights (IPR).

As the Office of General Counsel's technical assistance arm, CLDP upholds the Department of Commerce's mission, as stated in its 2018-2022 strategic plan to "Accelerate American Leadership." Strategic Objective 1.3 is "Strengthen Intellectual Property Protection," and one of the plan's strategies is to "strengthen the protection of intellectual property" abroad.

CLDP helps enforce IPR overseas through two types of technical assistance programs: programs that help countries develop an effective IPR enforcement environment, and programs that help countries create their own intellectual property, which gives them a vested interest in enforcing IPR.

Conducted in close cooperation with the USPTO, other Commerce bureaus, USTR, and other Federal agencies, CLDP's activities typically include consultations, seminars, workshops, and meetings.

Starting in March 2020, in light of the public health situation (COVID-19) and of the resulting impossibility to travel overseas, CLDP suspended its traditional activities, most of which took place overseas and conducted, instead, online video-conferences and webinars. At the suggestion of the Director of the USPTO's Global Intellectual Property Academy Director, GIPA and CLDP created an "IP eLearning Community of Practice" that has been effective in sharing lessons learned by both institutions as they conducted virtual programs.

In FY 2021, CLDP IP activities were conducted for the following countries and regions: Afghanistan, Algeria, Armenia, Bahrain, Bosnia and Herzegovina, Central Asia, Georgia, Middle East/North Africa, Pakistan, Sri Lanka, and Tunisia.

As outlined below, CLDP's FY 2021 activities mainly fell into four categories: Judicial Capacity Building in IPR Enforcement; Capacity Building for Institutions that Grant IPR; Capacity

Building for Institutions that Enforce IPR; and Development of Innovation Ecosystems, in particular through Technology Transfer.

OVERVIEW OF CLDP's FY 2021 IP PROGRAMS

1. Judicial Capacity Building in IPR Enforcement

Bosnia and Herzegovina:

CLDP Trains Judges on IP Adjudication to Improve the Rule of Law

On December 16, 2020, CLDP, along with USPTO and a U.S. federal judge, trained judges from the Centres for Judicial and Prosecutorial Training of the Republika Srpska and Federation of Bosnia and Herzegovina (BiH) on intellectual property (IP) adjudication. This session, the first in a three-part series, provided an overview of trademark and copyright law and highlighted the importance of IP protection. Training on IP adjudication is part of a larger effort to increase judicial capacity in BiH and strengthen the rule of law with respect to the information and communications technology sector.

CLDP Holds Civil Intellectual Property Adjudication Webinar

On February 3, 2021, CLDP, in coordination with U.S. Embassy Sarajevo, led a second webinar on intellectual property (IP) adjudication for judges and judicial staff in Bosnia-Herzegovina (BiH). This program is part of CLDP's ongoing effort to support BiH's ability to promote and protect IP rights. CLDP's assistance with judicial capacity building furthers the expansion of democratic institutions and facilitates fair and reciprocal trade and investment.

Adjudication of Intellectual Property Infringement Cases: Criminal IP Adjudication

On March 10, 2021, CLDP, in partnership with the Centre for Judicial and Prosecutorial Training of Federation of Bosnia and Herzegovina (BiH), conducted a one-day webinar which is the third installment in a series entitled Adjudication of Intellectual Property (IP) Infringement Cases and focused on criminal IP adjudication. Expert advisors included an Assistant U.S. Attorney from the Department of Justice (DOJ) whose presentation focused on DOJ's expertise in prosecuting computer crime and intellectual property. The main objective of the webinar was to foster a dynamic and interactive discussion between stakeholders of the BiH judiciary about the current state of criminal adjudication of IP cases.

2. Capacity Building for Institutions that Grant IPR

Afghanistan:

Trademark Webinar on Identification and Classification of Proposed Marks

On October 6 and 13, 2020, CLDP, in close cooperation with USPTO, conducted a two-part webinar for the Afghan Trademark Directorate (TMD) on trademark (TM) identification and classification as key elements in the examination of TM applications. This is the continuation of a series of webinars designed to increase the knowledge and skills of Afghan examiners,

enhancing the quality and consistency of operations at the TMD and creating value for both the consumer and seller.

CLDP Conducts Trademark Webinar on Registration Renewals

On January 26, 2021, CLDP, in collaboration with USPTO, conducted a two-hour webinar on trademark renewal for the TMD. Afghan officials participated in a discussion citing aspects of Afghan trademark law and raising issues faced by the TMD. The webinar included case studies meant to enhance the thoroughness, accuracy, and efficiency of the TMD in evaluating trademark registration renewal applications to be consistent with global best practices.

Trademark Examiners Review of Workshop Series

On March 31, 2021, CLDP, in close collaboration with USPTO, conducted a 2-hour webinar for the TMD to review the first eight workshops of the multi-series program on key aspects of trademark examination and registration, including distinctiveness, likelihood of confusion, classification, amendments, and renewals. The review consisted of a question and answer period, including pre-submitted, and ad hoc questions asked by TMD and answered by USPTO experts, as well as a follow-on discussion between and among TMD and USPTO participants.

Trademark Examination and Registration of Well-Known Marks

On April 22, 2021, CLDP, in close cooperation with the United States Patent and Trademark Office (USPTO), conducted a 2-hour webinar for the Afghan TMD focusing on the examination and registration of well-known marks. USPTO experts lectured on best practices relating to the examination and registration of well-known marks and used examples and case studies to reinforce the lecture materials. TMD staff were encouraged to ask questions as the lecture continued, including questions arising from TMD's experience in addressing issues related to well-known marks. This is the tenth virtual training session of a multi-part series focusing on key concepts and global best practices in the examination and registration of trademarks.

CLDP Conducts Webinar on Trademark Distinctiveness Hearing

On May 18, 2021, CLDP, in close cooperation with USPTO, conducted a webinar for the Afghan TMD to observe a hearing before the USPTO Trademark Trial and Appeals Board (TTAB) regarding trademark distinctiveness. CLDP prepared the participants with briefs of the issues at appeal and engaged the TTAB Chief Judge in private discussions with the participants to answer questions of law and practice prior to and post-hearing. By exploring the application of the key elements of distinctiveness and how a trademark application can be refused for being merely descriptive, this webinar builds upon the series of CLDP/USPTO webinars focused on critical elements of trademark examination and registration.

Georgia:

CLDP Leads Webinar Series on Intellectual Property

From October 5 to November 3, 2020, CLDP in cooperation with the USPTO and its Global Intellectual Property Academy, conducted a three-part virtual training series for the National Intellectual Property Center of Georgia (Sakpatenti). Topics for the training series included trade secret protection, telework practices and procedures, and overviews of the Trademark Trial and Appeal Board and the Patent Trial and Appeal Board. The training series included virtual

discussion sessions on each topic as well as related digitally recorded training videos for asynchronous learning. CLDP recorded each training video with Georgian language transcription and created an online video page in Georgian language so that the training materials could be accessed by interested staff members in the future.

CLDP Leads Consultation on Collective Management

On March 15-18, 2021, CLDP, in cooperation with the USPTO and the World Intellectual Property Organization (WIPO), led a webinar on collective copyright management with the National Intellectual Property Center of Georgia (Sakpatenti) and other IP stakeholders in Georgia. This webinar was designed to help develop solutions, in line with internationally accepted standards and best practices, to maintain an efficient system for fair and transparent collective copyright management in Georgia. Georgia has been a model for collective management in the Caucasus and Central Asian region, but due to recent developments in the collective management field, rightsholders and users are confused about the Collective Management Organizations (CMO) system and concerned about royalty collection and distribution. As part of this intervention, CLDP arranged for an expert in copyright and collective management to review Georgia's Law on Collective Management of Copyright and Related Rights and provide a gap analysis to Sakpatenti. CLDP then drafted and delivered to Sakpatenti a Post-Program Report with Recommendations. Both documents will assist Sakpatenti in building support and consensus around the steps needed to strengthen the current system. CLDP is prepared to assist with the organization of follow-up activities in collaboration with Sakpatenti.

3. Capacity Building for Institutions that Enforce IPR

Central Asia:

CLDP Presents on Socio-Economic Aspects of Trade in Counterfeits

On November 17, 2020, CLDP participated in a webinar hosted by the American-Uzbekistan Chamber of Commerce on the prevention of counterfeits for customs officials from the Kyrgyz Republic, Tajikistan, and Uzbekistan. This webinar aimed to strengthen Central Asian countries' intellectual property (IP) rights, laws, and policies to ensure a more level playing field for IP stakeholders in the region.

CLDP Holds Second Meeting of the Central Asia Expert Level Working Group on Intellectual Property Rights (IPR)

On January 27, 2021, CLDP, in partnership with the National Intellectual Property Rights Coordination Center, USTR, and USPTO, hosted a webinar for the Central Asia Regional Expert Level Working Group on Intellectual Property (IP) Rights concerning interagency coordination for the protection and enforcement of IP rights. The webinar gathered participants from all five Central Asian Republics and discussed processes and best practices for successful interagency coordination in IP enforcement. A set of recommendations were developed and, once finalized, will be sent for country adoption as well as U.S.-Central Asia Trade and Investment Framework Agreement (TIFA) and C5+1 Platform adoption. CLDP's technical assistance to the Central Asia IP Working Group seeks to strengthen and improve IP protections in order to increase foreign direct investment and trade in the region.

CLDP Leads U.S.-Central Asia TIFA Working Groups Session

On March 29, 2021, CLDP led the working group session of the U.S.-Central Asia Trade and Investment Framework Agreement (TIFA) Council meeting. CLDP reported on the work of its Expert Level Working Groups on Customs, Women's Economic Empowerment, Sanitary/Phytosanitary Measures, and Intellectual Property Rights (IPR). The TIFA Working Groups unanimously adopted CLDP's recommended focus areas and projects for the current year, which CLDP developed in coordination with the U.S. Government interagency and with foreign counterparts. Despite recent improvements, two Central Asian countries, Turkmenistan and Uzbekistan, remain on the U.S. Trade Representative's Special 301 Watch List. By working with the Expert Level Working Group on IPR to implement the TIFA Council's IP-related recommendations, CLDP will help further the Working Group's goal to strengthen intellectual property rights and their enforcement in the region, including through increased coordination nationally and internationally, and thereby to contribute to increased regional trade and investment.

CLDP Holds Third Meeting of the Central Asia Expert Level Working Group on Intellectual Property Rights (IPR)

On July 14-15, 2021, CLDP virtually gathered government experts from Kazakhstan, the Kyrgyz Republic, Tajikistan, Turkmenistan, and Uzbekistan with U.S.-based interagency advisors. The meeting provided a unique platform for interactions among the Central Asian experts and set up a series of meetings to address and overcome deficiencies in intellectual property rights (IPR) protections in Central Asia, as noted in the U.S. Trade Representative's Special 301 Report. Aligning IPR protections and enforcement in Central Asia with international best practices will promote innovation and economic diversification and will lead to increased trade and investment in the region.

Pakistan:

CLDP Conducts Webinar on Combating Counterfeits

On February 16, 2021, CLDP, in close cooperation with the U.S. Food and Drug Administration (FDA) and USPTO, conducted the second webinar in a series focusing on the prevention of counterfeit medicines and medical devices. The audience was composed of 80 representatives from Pakistan's Federal Bureau of Revenue-Customs (FBR), representing five internal FBR Directorates (Intellectual Property Rights Enforcement, Model Customs Collectorate, General Intelligence & Investigation, General Audit and Adjudication, Enforcement and Compliance). This program aims to enhance the skills of FBR officials responsible for enforcing intellectual property rights by stopping the import and export of counterfeit goods at the border, contributing to the protection of the health and safety of the general public.

Exchange of Best Practices on Combating Counterfeit Medical Products (Modules 1&2)

On March 30 and April 6 & 13, 2021, CLDP, in close cooperation with USPTO, FDA, HSI, and the U.K. Border Force (UKBF), continued the program of exploring best practices to combat counterfeit medicines and medical devices at a country's borders. Module 1 was completed over a four-week period beginning February 9th, and Module 2 consisted of two 2-hour virtual sessions, with one session per week focused on the concerns, experiences, perspectives, interests, and best practices of the pharmaceutical and medical device industry in Pakistan and across the

globe. The program was for Pakistan officials involved in the protection of Pakistan's drug supply from the threat of counterfeits transiting through air freight and air mail facilities in Pakistan. This program was a follow-on to CLDP and USPTO programs with FBR (Customs), IPO and the judiciary regarding customs enforcement and IP-related matters, all of which strengthen Pakistan's IP rights enforcement regime, as well as protecting the public health and safety from dangerous counterfeit products.

Exchange of Best Practices on Combating Counterfeit Medical Products (Module 3)

On July 13 & 27 and August 24 & 31, 2021, CLDP, in close cooperation with USPTO and FDA, continued the multi-series virtual program focused on exploring best practices to combat counterfeit medical products at a country's borders. Module 3 consisted of four 2-hour virtual sessions focused on the capabilities of USCBP, the UKBF, and FBR (Customs) to halt the scourge of counterfeit products transiting across multiple country borders; highlighted the intelligence collection, targeting, insider threat, and import control capabilities of the UKBF; and emphasized best practices for international/interagency collaboration, including case studies of successful U.S.-U.K. cooperation.

4. Development of Innovation Ecosystems/Technology Transfer

Algeria:

CLDP Conducts Webinar on Academia-to-Industry Technology Transfer

On November 18, 2020, CLDP, in collaboration with Algeria's technology transfer agency (ANVREDET), conducted a webinar focused on strategies for effective technology commercialization. The webinar focused on key components of academia-to-industry technology transfer ecosystems, including developing intellectual property policies and creating university technology transfer offices. CLDP's collaboration with ANVREDET is part of CLDP's ongoing effort to promote innovation and entrepreneurship in Algeria, through technology transfer and intellectual property rights.

CLDP Conducts Intellectual Property Workshop for University Start-Ups

On June 14-15, 2021, CLDP, in partnership with Algeria's ANVREDET, conducted a virtual workshop for managers of university incubators across Algeria. With representatives from U.S. Embassy Algiers and the European Union in attendance, the workshop presented and discussed international best practices for the protection and valuation of intellectual property (IP) assets created at university start-ups. The USPTO IP Attaché for the MENA region was the key speaker for the first day of the workshop, focused on IP protection. CLDP was the key speaker for the second day, focused on valuation. The development of technology start-ups has become a priority for the Algerian government, as it seeks to transition to a knowledge-based economy and shift away from reliance on oil and gas.

New Technology Transfer Office Created with CLDP Assistance

On August 9, 2021, the National Polytechnic School of Algiers (ENP) informed CLDP that ENP had created its first technology transfer office (TTO) as a result of CLDP assistance. For the last five years, CLDP has supported the innovation ecosystem in Algeria through capacity building technical assistance focused on technology transfer and intellectual property. TTOs are an

essential tool for bringing innovation from academic research to market through the protection and licensing of intellectual property.

CLDP Co-Organizes, and Presents at Workshop on *The Viability of Advanced Technology Start-ups*

The development of advanced technology start-ups (ATS) is a priority for the Algerian government, as it will be a key condition of the country's transition from a resource-based economy to a knowledge-based economy. The U.S. embassy in Algeria supports this priority because it will contribute to better enforcement of intellectual property rights. In light of the embassy's position, CLDP proposed to join forces with the Algerian Information Technology Association (AITA) to organize a workshop focused on ways to ensure the viability of ATS. The embassy agreed and the Algerian government, at the highest level, embraced this initiative.

On October 5-6, 2021, a workshop focused on *The Viability of Algerian Advanced Technology Start-ups* took place in Algiers. This workshop – co-organized by CLDP, AITA, and Algerian government institutions – had more than 100 participants, including government officials, managers of technology incubators, and members of start-ups. A delegation from the U.S. embassy attended the workshop, with CLDP joining virtually. CLDP gave a presentation on the methodology it has created to assess the viability of ATS; the Algerian government co-organizers, in a written message, praised this presentation.

In coming months, as a follow-up to the workshop, three “train the trainers” pilot programs will be launched at the behest of the U.S. embassy to build Algeria's capacity to support ATS. One of these pilot programs, focused on IP protection strategy, will be conducted by USPTO's IP Attaché for the MENA region.

Armenia:

Videoconference on Technology Transfer

On March 23, 2021, CLDP, in coordination with the U.S. Embassy in Yerevan, held a videoconference with a multi-stakeholder group of government officials and private sector leaders to discuss technology transfer capacity and the potential for commercialization of intellectual property at universities and research institutions in Armenia. The videoconference highlighted the progress of a group of university and legal professionals in establishing a technology transfer office in Armenia following their participation in CLDP-led technical assistance programs on technology transfer in 2017 and 2018. Technology transfer and commercialization of intellectual property promote innovation and economic development and create opportunities for future research and development partnerships with American institutions.

Bahrain:

CLDP Helps Develop Technology License Template for Technology Transfers

Over the last year, CLDP, in cooperation with USPTO's IP Attaché for the MENA region, helped the Kingdom of Bahrain create the Bahrain Innovation and Technology Center (BITC), now known as the Bahrain Innovation and Technology Transfer Center (BITTC). BITTC is located at the University of Bahrain and serves all nine universities of the Kingdom. BITTC's

key mission is to transfer new technologies developed by universities to the private sector through technology licensing agreements. In December 2020 and January 2021, CLDP collaborated with BITTC to develop a template for technology license agreements. This template addresses key risks the Kingdom's universities face in technology transfers and ensures they will derive proper revenues from such transfers.

CLDP Creates Country-Specific Invention Disclosure Forms for BITTC

On February 17, 2021, CLDP, USPTO, and technology-transfer advisors conducted a video conference call to finalize Bahrain-specific Invention Disclosure Forms (IDFs). Bahrain university professors can use the IDFs to inform BITTC of their inventions. This enables BITTC to seek Intellectual Property (IP) protection in the form of patents and support the commercialization of the inventions through licensing. Technology-transfer entrepreneurship will assist the country with diversifying its economy and create investment opportunities for both Bahraini and U.S. businesses. This effort is part of a larger initiative undertaken by CLDP at the request of the U.S. Embassy in Bahrain, to assist the country with the creation of BITTC, IP policy, technology transfer methodologies, and technology licensing templates. CLDP conducts this work in coordination with the USPTO Attaché for the MENA region.

CLDP and USPTO Train BITTC Staff in IPR

On March 15 and 24, 2021, CLDP, in close collaboration with the USPTO, trained BITTC staff on patent filing in the Gulf Cooperation Council. This program is part of a CLDP-USPTO collaboration to conduct over 40 hours of intellectual property rights (IPR) training for BITTC. The program also included training on how to obtain patents and copyrights in the United States as well as other jurisdictions.

CLDP Provides Training to Technology Transfer Office

On May 18 and 20, 2021, CLDP provided to BITTC staff a two-day training workshop led by U.S. technology transfer academics and professionals. The training workshop focused on the ways to manage technology innovations at university-based technology transfer offices, including how to research patents related to innovation ideas from Bahraini students and faculty. Representatives from George Mason University and Cornell University will provide additional mentoring meetings to BITTC staff during the academic year as questions arise. Effective innovation support from BITTC will allow Bahraini entrepreneurs to protect and commercialize their innovations globally, and potentially partner with U.S. entrepreneurs in the process.

CLDP Conducts Simulated Technology Licensing Negotiations for BITTC

On June 1, 2021, CLDP conducted a simulated technology licensing negotiation exercise for BITTC's staff. This exercise was based upon a case study created by CLDP, and the former director of Cornell University's technology transfer office engaged in simulated technology licensing negotiations with BITTC's staff. This program developed the capacity of BITTC staff to commercialize patented inventions through technology licensing.

CLDP Helps Hone Technology Licensing Negotiations Skills of BITTC Staff

On June 16-17, 2021, CLDP conducted a more complex simulated technology licensing negotiation exercise, with BITTC being now in the position of a potential licensor. This exercise was based upon a case study created by CLDP to simulate technology transfer licensing

agreement negotiations in the healthcare industry, thereby further developing BITTC staff's capacity to commercialize inventions through technology licensing.

CLDP Conducts Workshop on Technology Licensing to Spin-offs

On June 23, 2021, CLDP conducted a workshop for the BITTC that simulated negotiations on the licensing of technology to spin-offs. Spin-offs are start-up companies that commercialize inventions created by university faculty members. Under intellectual property (IP) policies of the Bahraini universities serviced by BITTC, the IP rights of spin-offs belong to the faculty's university. This workshop was based on a case study created by CLDP and a U.S. patent lawyer who negotiates with BITTC.

CLDP Conducts Webinar on Material Transfer Agreements

On July 14, 2021, CLDP conducted a webinar on Material Transfer Agreements (MTAs) for BITTC. MTAs are contracts that govern the transfer of materials between an organization that possesses rights in the material and an organization that plans to use the material for research. MTAs are very important for biological research, and therefore, for subsequent technology transfer. A former director of Cornell University's Technology Transfer program provided the presentation for BITTC staff. The BITTC assists university professors and students from all nine universities in Bahrain to collaborate with businesses to commercialize technology innovations from Bahrain.

CLDP Conducts Mentoring Session for BITTC Staff

On July 27, 2021, CLDP conducted a mentoring session focused on inventiveness analysis for Bahrain's Innovation and Technology Transfer Center (BITTC) staff. Utilizing the expertise of the former director of Cornell University's Technology Transfer Office, these mentoring sessions are designed as small group question and answer sessions, complementary to the workshops conducted by CLDP and USPTO's IP Attaché for the MENA region. CLDP will host similar sessions once a month with the goal of increasing BITTC's staff effectiveness and assisting start-ups in Bahrain.

Middle East/North Africa Regional:

Empowering Women Entrepreneurs through Business and Legal Strategies in the Technology Era

On March 22-25, 2021, CLDP, in partnership with Tunisia's National Agency for the Promotion of Research, organized a series of webinars on empowering women entrepreneurs from the Middle East and North Africa (MENA) region and Azerbaijan. The regional conference brought together women entrepreneurs and innovators, government officials, and international institutions to discuss commercial and business tools available to support women-owned technology businesses. The conference was divided into four modules focused on intellectual property, legal resources, commercial strategies, and business strategies to help women build and run successful businesses.

Pakistan:

Technology Transfer Conference

On March 15-19, 2021, CLDP, in close cooperation with the Higher Education Commission of Pakistan (HEC), sponsored 15 managers from university offices of research, innovation, and commercialization (ORICs) and business incubation centers (BICs) to virtually attend the Association of University Technology Matters (AUTM) 2021 Annual Meeting and Conference. The AUTM conference is the world's largest gathering of technology transfer professionals. The conference was structured to be highly interactive, with program sessions focused on learning, networking, and deal-making with over 1,500 professionals from 20 different countries and the leading universities around the world. Some of the topics covered included drafting and negotiating intellectual property (IP) license agreements, industry -academic partnerships, innovation strategies, administration of technology transfer offices, "nuts and bolts" of technology transfer, IP trends and successful practices, innovation focusing on agriculture, and proof of concept and early stage technologies. This program continues to build on programs conducted by CLDP with HEC and others, all of which contribute to the strengthening of Pakistan's IP regime.

CLDP Continues Engagement with Georgetown Law Center TradeLab

On April 30, 2021, Georgetown Law Center's TradeLab Practicum student team gave a presentation to CLDP and interested Georgetown faculty and students on their research, analysis, and recommendations regarding intellectual property (IP) rights enforcement in Pakistan. CLDP had previously directed the student team to investigate the authorities, composition, resourcing, and effectiveness of Pakistan's special IP tribunals/courts. The student team conducted virtual interviews with lawyers, judges, and businesses operating in Pakistan to gain an on-the-ground perspective of the challenges facing IP rightsholders in Pakistan. To better assess these tribunals/courts, the students conducted comparative research on other special tribunals/courts in six different countries and prepared a matrix of their strengths and weaknesses. This research helped the student team to formulate and recommend improvements to the laws, the tribunals/courts, and to the overall IP rights protection regime in Pakistan. The final written memorandum was presented in mid-May, and CLDP will consider the recommendations of the student team in the development of future programming on IP rights enforcement in Pakistan.

Sri Lanka:

CLDP Begins a Series of Technology Transfer Webinars

On December 2 and 4, 2020, CLDP, in partnership with USPTO, conducted the first two sessions of a multi-phase virtual program on technology transfer in Sri Lanka. CLDP developed this program at the request of the Sri Lanka Ministry of Education as a follow-on to an earlier CLDP program for the senior managers of newly formed university technology transfer offices (TTOs). Experts from the University of Michigan and USPTO presented a variety of subjects including the roles and responsibilities of TTOs, the impact of the U.S. Bayh-Dole Act, developing and sustaining relationships with the business sector, and the recognition, evaluation, protection, and commercialization of intellectual property (IP) resulting from university research. This program will strengthen the capabilities of the country's TTOs and highlight the key role of IP in creating and sustaining innovation ecosystems that generate economic and societal benefits.

Technology Transfer Conference

On March 15-19, 2021, CLDP, in close cooperation with the Sri Lanka Ministry of Higher Education (MoHE), sponsored 21 managers from University Business Linkage offices (UBL cells) to virtually attend the Association of University Technology Managers (AUTM) 2021 Annual Meeting and Conference. (The AUTM conference is discussed above, in the first item for Pakistan.) This program continues to build on programs conducted by CLDP with MoHE and others, to establish and enhance UBL cells at public and private universities across Sri Lanka, all of which play a key role in creating and maintaining an ecosystem of innovation and contribute to the strengthening of Sri Lanka's IP rights enforcement regime.

Webinar Series on Technology Transfer

On September 28, 2021, CLDP, in cooperation with USPTO, provided a 3-hour virtual program for university technology transfer offices on the University–Industry relationship, consisting of a 90-minute prerecorded lecture to be followed by a 2-hour live virtual program with experts from the office of Michigan State University (MSU) Technologies. The prerecorded program was provided in advance to encourage the participants to study the materials, discuss within their university teams, and submit questions for the live/interactive second portion of the program. MSU experts focused on the suite of agreements that define the business relationship and protect the parties (including confidentiality agreements, research agreements, material transfer agreements, and licensing agreements) and explored the critical needs and goals of businesses and universities relating to the commercialization of newly developed intellectual property (IP). A lecture format was utilized, with learnings reinforced and supplemented by examples, case studies, and exercises. Subsequent webinars will focus in detail on various subjects critical to the successful commercialization of IP, such as key provisions in licensing agreements, establishing start-ups, and other forms of technology transfer.

Tunisia:

CLDP Conducts Webinar at National Conference on Technology Transfer

On November 4, 2020, CLDP, at the request of the Tunisian Agency for the Promotion of Research (ANPR), conducted a webinar for technology transfer stakeholders on strategies for technology commercialization. Participants discussed key commercialization topics for Tunisia such as developing institutional capacity to manage intellectual property assets, seeking patent protection internationally, and determining the value of new technologies. CLDP's collaboration with ANPR is part of its ongoing technical assistance to Tunisia under the Middle Eastern Partnership Initiative of the U.S. Department of State.

Ukraine:

Kickoff of IP National Moot Competition

On September 20-21, 2021, CLDP, in cooperation with the Ukrainian Bar Association, USPTO's IP Attaché in Ukraine, the U.S. Foreign Commercial Service, and USAID's New Justice Program, conducted a seminar for Ukrainian law students on the basics of the intersection between IP law and commercial contract law. This event kicked off a year-long project that will see Ukrainian law students analyze, write about, and argue issues related to a series of moot IP and commercial law issues. The final competition and accompanying conference will take place

in Kyiv on World IP Day in April 2022. This initial event introduced students to fundamental concepts in IP law, both at the domestic and international levels, and provided lessons on best practices in oral advocacy and legal writing. The program will help to ensure that a new generation of Ukrainian lawyers enter the work force with a deepened understanding of, and appreciation for, IP rights enforcement and protection.

Intellectual Property Moot/Licensing Webinar

On December 15-17, 2021, CLDP and a group of stakeholders conducted a series of interactive lectures and trainings for Ukrainian law students. This builds on a September in-person training for students that introduced them to high-level concepts in IP law. The program focused more specifically on domestic and international legal concepts surrounding licensing agreements. In addition to substantive topics, students heard from practicing IP attorneys about various careers in the field. The webinar is part of CLDP's Ukraine IP moot initiative aimed at increasing interest and appreciation for IP law and protection among Ukrainian law students.

INTERNATIONAL TRADE ADMINISTRATION (ITA)

Office of Standards & Intellectual Property (OSIP)

STOPfakes.gov

The International Trade Administration's Office of Standards and Intellectual Property (OSIP) manages the STOPfakes.gov program including resources provided on the STOPfakes website. STOPfakes.gov hosts digital materials which seek to educate and assist businesses, consumers, government officials, and the general public.

Industry Specific IP Toolkits

These industry sector toolkits focus on IP and provide guidance to U.S. companies seeking to acquire, use and protect copyrights, patents, trademarks, and trade secrets in overseas markets. Current industries covered include Sporting Goods, Marine Technology, Pleasure Boats, Medical Devices, Auto Parts, Building Products, and Smart Mobility.

IP Snapshots

IP Snapshots are one-page documents that provide IP information about a foreign country. The following information is included on each IP Snapshot: Contact information for local IP Offices, country membership in important IP treaties, the USTR Special 301 Report rankings for the prior three years, and contact information for the IP attaché in the region. Seventy-nine (79) IP Snapshots are currently available on STOPfakes.gov.

Country IP Toolkits

Country Toolkits seek to assist U.S. entrepreneurs with thorough country specific insight focused on IP protections in foreign markets. Available toolkits include China (updated), Singapore, Korea, Malaysia, Vietnam, Thailand, Brunei, Brazil, Colombia, Egypt, European Union, Italy, and Peru.

IP Highlights

These digital resources raise awareness on a range of IP related issues. The inaugural *IP Highlight* was on *Suspicious Solicitations*, and it noted how bad actors negatively impact rightsholders by impersonating government agencies. Additionally, the *IP Highlights* provide information on an array of U.S. Government IP Resources, including the IP Attaché Program, the Interior Department's Indian Arts and Crafts Board, Enforcement on Counterfeit Car Seats, and the USPTO's Patent Pro Bono Program.

STOPfakes Roadshows

The [STOPfakes Roadshows](#) deliver critically important information about intellectual property to the audiences that need it most – start-ups, entrepreneurs, small and medium-sized businesses, independent creators, and inventors. The information is presented by experts from multiple government agencies focused on advancing stakeholders' intellectual property interests:

- The U.S. Patent and Trademark Office provides information about how to protect patents and trademarks;
- The U.S. Copyright Office discusses the importance of copyright protection to creators and businesses;
- U.S. Customs and Border Protection (CBP) explains how a registered trademark or copyright can be recorded with CBP to facilitate the seizure of infringing goods at our borders;
- The Federal Bureau of Investigation (FBI) or a U.S. Attorney's Office discusses how to protect trade secrets and identify internal and external threats;
- The U.S. Department of State highlights the role diplomacy and our diplomatic missions play in advocating for U.S. businesses overseas;
- The International Trade Administration identifies mechanisms for obtaining intellectual property rights protections in export markets; and
- The Small Business Administration advises on the potential use of grants and loans to help with the costs of obtaining IP protection before exporting.

Participating agencies also identify additional resources they make available to assist U.S. businesses with acquiring and protecting their intellectual property rights.

In 2018, the STOPfakes team expanded the opportunities available to businesses at the “in-person” roadshows through what are now its three signature offerings: First, participants were able to sign up to talk one-on-one with any of the government agency speakers during 10-minute sessions. Second, participants could apply for online copyright registration. Copyright Office staff offered on-site assistance with the copyright application process. Third, participants were able to apply for copyright and trademark recordation. On-site assistance was made available by Customs and Border Protection staff to navigate the recordation application portal and process.

Given the current pandemic, the in-person roadshows have been paused. In FY 2021, in place of the roadshows, OSIP offered several innovative virtual STOPfakes webinars.

STOPfakes Webinars

STOPfakes began offering virtual content in August 2020 with eleven webinars taking place between August 25, 2020, and September 30, 2021. For FY 2021, OSIP continued its virtual STOPfakes webinars with a total of four webinars. These webinars are hosted by STOPfakes and feature some of the same topics and speakers from the roadshow agendas as well as some content from new partners (e.g., NHTSA discusses product safety issues with counterfeit airbags, car seats, replacement parts, etc.). The webinars are being recorded and will be posted on the STOPfakes website and announced via the STOPfakes Twitter feed.

The topics covered in the FY 2021 virtual STOPfakes Webinars included:

- *IPR Border Enforcement: Recording Trademarks and Copyrights with CBP*
- *Trademark Basics: What Every Small Business Should Know Now, Not Later with USPTO*
- *Patent Basics and USPTO Resources: What Every Small Business Should Know When Developing their Business Plan and Moving Forward*
- *Registering Your Trademark Internationally*

IP Consultations for Businesses and Associations

OSIP provided IP business guidance and insight for entities as they sought to expand their opportunities for exporting. Additionally, OSIP participated as a panelist on webinars for associations seeking to provide IP information for their association members.

Combating Trafficking in Counterfeit and Pirated Goods

OSIP undertook a critical role in the interagency process to develop and implement the January 2020 Report by the Department of Homeland Security on *Combating Trafficking in Counterfeit and Pirated Goods*. In FY 2021, OSIP continued to meet regularly with industry leaders and

provide industry's unique perspective as part of OSIP's support for the ongoing USG activities to combat trafficking in counterfeit and pirated goods.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

Protect Intellectual Property at ICANN

The National Telecommunications and Information Administration (NTIA), USPTO, and other Federal agencies, including the Federal Trade Commission and the Department of Justice, continue to engage within the Internet Corporation for Assigned Names and Numbers (ICANN) and the Governmental Advisory Committee (GAC), highlighting the importance of timely access to domain name registration information (known as WHOIS) for IP rightsholders, to combat infringement online. In response to the European Data Protection Regulation (GDPR), which went into effect during 2018, crucial domain name registration information details are no longer publicly provided. The U.S. Government is playing an active role in the ongoing ICANN policy development process discussions to establish a sustainable access and accreditation model as soon as possible, so that IP rightsholders and other legitimate interests can access non-public WHOIS information for enforcement and security purposes. The U.S. Government will continue to work through the GAC to ensure that intellectual property rights are respected in the ICANN policy development processes.

In addition, the review of the new rights protection mechanisms (RPMs), such as the Trademark Clearinghouse, Trademark Claims Service, and the Uniform Rapid Suspension System, has been completed and awaiting ICANN Board review. The RPMs were created to address intellectual property concerns in response to the introduction of new top-level domains. NTIA, USPTO, IPEC, and other interagency colleagues closely monitored the review of the RPMs and will continue to focus on the effectiveness of these new RPMs. USG also will be closely following the review of the Uniform Domain Name Dispute-Resolution Policy (UDRP), which is expected to begin in 2022. Since its introduction in 1999, the UDRP has been a successful tool in assisting trademark rightsholders to combat cybersquatting.

The Section 1201 Rulemaking

Throughout FY 2021, NTIA followed developments in the eighth triennial rulemaking proceeding under 17 U.S.C. § 1201(a)(1)(C), which concluded in October 2021. The rulemaking process allows the Librarian of Congress to determine whether the Librarian should grant any temporary exemptions to the prohibition on circumvention in 17 U.S.C. § 1201(a)(1). NTIA worked to fulfill its statutory role to engage in consultation with the U.S. Copyright Office during the rulemaking. NTIA reviewed the proposals and additional comments received in the process. At the invitation of the Copyright Office, NTIA also participated in the Office-led public hearings in April 2021 to ask questions to supporters and opponents of the various proposals. NTIA formally shared its views with the Copyright Office through an extensive consultation letter transmitted on October 1, 2021.

NTIA appreciates the positive process changes that the Copyright Office has continued to implement in the rulemakings, several of which track closely with recommendations NTIA has made both in its previous consultations and in less formal discussions. For example, although necessitated by the ongoing COVID-19 pandemic, NTIA found remote participation at the public hearings to be a success, as it allowed for more inclusive public participation in the process.

UNITED STATES PATENT AND TRADEMARK OFFICE (USPTO)

The Director of the USPTO has the responsibility of, among other things, advising “the President, through the Secretary of Commerce, on national and certain international intellectual property policy issues” and advising “Federal departments and agencies on matters of intellectual property policy in the United States and intellectual property protection in other countries.” 35 U.S.C. § 2(b)(8)-(13). Consistent with this responsibility, the USPTO provides expert legal and policy advice to the Administration on issues related to the protection and enforcement of patents, industrial designs, trademarks and geographical indications, copyrights, plant varieties, and trade secrets, including regulatory test data.

The USPTO represents the United States at the World Intellectual Property Organization (WIPO) and in other international intergovernmental organizations that discuss IP-related matters. In addition, during FY 2021, the Department of Commerce – including the USPTO – provided advice to the Office of the United States Trade Representative (USTR) through extensive input into: the annual Special 301 review of global IP regimes; the Economic and Trade Agreement between the government of the United States of America and the government of the People’s Republic of China, including by providing written comments and recommended changes for dozens of implementing measures under Chinese law and participating in technical level calls with Chinese counterparts to discuss implementation obligations; trade agreement negotiations with the government of Kenya and the government of the United Kingdom; and the Notorious Markets Review, as well as the Section 301 investigations when intellectual property issues are involved. Additionally, the USPTO participates in the Asia-Pacific Economic Cooperation (APEC) Intellectual Property Experts Group (IPEG) meetings and advises USTR on IP enforcement-related issues in the context of APEC initiatives. The USPTO provides advice on initiatives, reports, proposed programs, and developments related to IP enforcement made or produced by other APEC economies. The USPTO also organizes and conducts IP enforcement-related programs/seminars for APEC economies.

Throughout FY 2021, USPTO’s OPIA conducted a state sovereign immunity study in response to an inquiry from Senators Thom Tillis and Patrick Leahy. Specifically, OPIA performed case law research and statistical studies, and submitted its report to Congress on August 31, 2021 (<https://www.uspto.gov/sites/default/files/documents/USPTO-Report-to-Congress-August2021.pdf>).

Strengthen Intellectual Property Enforcement through International Organizations

The USPTO continues to lead the U.S. delegation to the WIPO Advisory Committee on Enforcement (ACE). ACE provides a multilateral forum for exchanging information and best

practices on combatting trademark counterfeiting and copyright piracy. In September 2021, the USPTO's OPIA participated in and chaired the ACE Online Dialogue, which featured presentations from all WIPO regional groups on New Developments in Combatting Counterfeiting and Piracy on the Internet.

The USPTO has also entered into a number of arrangements with intergovernmental organizations. For example, the USPTO's Memorandum of Understanding (MOU) with INTERPOL's Illicit Goods and Global Health Programme has been renewed through 2023. Under the arrangement, the USPTO and INTERPOL intend to cooperate on training and capacity building programs to promote effective intellectual property enforcement internationally. The USPTO also entered into an MOU with the Oceania Customs Organization (OCO), which is composed of 23 national and territorial customs administrations in the Pacific region. The MOU, which runs through September 2023, provides that the OCO and the USPTO intend to cooperate on training and capacity-building programs to promote effective intellectual property enforcement in the region.

Promote Enforcement of U.S. Intellectual Property Rights through Trade Policy Tools

Throughout FY 2021, the USPTO provided policy advice and technical expertise on domestic and international IP matters to multiple other federal agencies. These included USTR, IPEC, and other bureaus of the Commerce Department. The USPTO also advised USTR on reviews under U.S. trade preference programs such as the Generalized System of Preferences and the African Growth and Opportunity Act (AGOA); Trade Policy Reviews undertaken at the World Trade Organization (WTO); amendments to the South Africa copyright and performers laws; a draft Nigerian copyright bill; the Ukrainian collective management organization (CMO) law and CMO issues; the Indian copyright law; Singapore's copyright law reform; Thailand copyright law amendments; Vietnam's IP law amendments; Mexico's new copyright law and its USMCA obligations; and accessions underway at the WTO. In addition, the USPTO assisted USTR in the preparation of its annual review of global developments on trade and IP and the Special 301 Report. The Special 301 Report identifies U.S. trading partners in which IP protection and enforcement has deteriorated or remained at inadequate levels and where U.S. persons who rely on IP protection have difficulty with fair and equitable market access. The USPTO assisted in its preparation by providing extensive information on the state of IP protection and enforcement in 70 countries under review. The USPTO likewise provided USTR with information in connection with its compilation of the annual Notorious Markets List, which highlights prominent online and physical marketplaces that reportedly engage in and facilitate substantial copyright piracy and trademark counterfeiting.

Support U.S. Small and Medium-Size Enterprises (SMEs) In Foreign Markets

The USPTO offers basic- and advanced-topic programming for U.S. Small and Medium Sized Enterprises (SMEs) doing business abroad through its Global Intellectual Property Academy (GIPA), a component of the Office of Policy and International Affairs (OPIA). These in-depth programs – organized and conducted by OPIA attorneys – cover best practices in domestic and international IP protection and enforcement and are typically delivered through face-to-face and distance learning modes, both from the USPTO's headquarters in Alexandria, VA, and around

the country in cooperation with the USPTO's regional offices and other business units. OPIA collaborates with the USPTO's IP Attachés, Regional Offices, other USG agencies, and the Federal Judiciary. In FY 2021, GIPA provided IP awareness and education programming to over 7,740 U.S. SMEs, U.S. government officials, and other U.S. stakeholders. About 22% of GIPA's 248 programs in FY 2021 targeted this domestic audience of IP rights owners, users, and policymakers. During FY 2021, GIPA continued its successful 2020 pivot to all-remote outreach and education delivery, thanks to prior investments in technology platforms and e-learning strategies.

During FY2021, the USPTO continued its China IP Roadshows, a series of one-day events that delve into the details of how to better protect IP in China. The Roadshows bring to local businesses and stakeholders the expertise and knowledge of the USPTO's China specialists as well as that of special invited guests, who often include local businesspeople and IP experts, thus tailoring the programs to the needs of the specific locales in which they are held. In FY 2021, the USPTO also supported the interagency STOPfakes.gov Initiative, which generally included organizing and staffing IP Roadshows and webinars throughout the country and maintaining and updating IP Toolkits, including the China IPR Toolkit and a set of *IP for SME* toolkits for U.S. and UK small-and medium-sized enterprises, which are posted to the USPTO.gov and STOPfakes.gov websites. The USPTO through OPIA/GIPA continued certain domestic training and outreach initiatives, converting previously in-person programming to the virtual environment for several audiences, including IP education programming for U.S. state attorneys general in cooperation with the National Association of Attorneys General (NAAG), joint programs with universities and China IP Roadshows and Webinars for U.S. SMEs, as well as a virtual pilot program on IP for U.S. SMEs doing business in Southeast Asia. USPTO continued a successful multi-year webinar initiative to provide comprehensive IP education to grantees of the Small Business Administration's (SBA) SBIR-STTR programs; participated in the SBA Office of Trade webinar on *Learn About Trade: Protecting Your IP in Trade*; supported small business advisors by providing international IP protection and enforcement training sessions in the international trade track and plenary at the annual America's Small Business Development Center (ASBDC) conference; and offered a program on copyright basics and considerations for entrepreneurs for several Small Business Development Centers (SBDCs) located in Massachusetts, Washington, DC, Puerto Rico, and Texas. The USPTO supported DOC and whole-of-government efforts to support Women's Economic Empowerment (WEE) through providing IP subject matter expertise to WEE programming. USPTO participated in CLDP and ITA WEE programming, including the ITA's August 2021 virtual event on *Women Empowered Leave Legacies Through Trade & Investment (WELLTI) Coffee Chat: Disruptors & Innovators: Women in STEM*, which was marketed to women in the U.S. who are in the STEM field interested in doing business in South Africa.

Raise Public Awareness of International Intellectual Property Protection and Enforcement

The USPTO engages in many outreach activities to raise public awareness of IP. Knowledge is shared through libraries and resource centers, universities, regional offices, face-to-face and distance learning educational programs, and through presence at trade shows. Additionally, content covering all areas of IP is available on the [USPTO's website](#) and promoted through the USPTO's social media platforms.

In FY 2021, GIPA continued its decade-long commitment to produce on-demand content through distance-learning modules on the USPTO website. These modules are available in five languages and cover six different areas of IP protection. In addition, self-study materials – including recordings of events, training slides, and IP toolkits – were updated for asynchronous learning. This on-demand content collectively has drawn nearly 200,000 unique views since their launch in 2010, with the most recent videos covering Patents and Trade Secrets receiving a combined 68,345 views.

The USPTO also participates frequently in programs to engage directly with innovators, students, and entrepreneurs. For example, in February 2021, USPTO’s OPIA hosted a virtual international forum on the protection of industrial designs, focusing on global trends and developments around the globe.

During March 2021, the USPTO conducted its annual Women’s Entrepreneurship Symposium through a series of virtual programs; and on August 18-20, the USPTO conducted the 2021 Invention-Con online.

On March 30, 2021, the USPTO’s OPIA enforcement team launched a new phase of its *Go For Real Anti-Counterfeiting Campaign* with the roll out of the digital *Dupe Detector Kit*, a state-of-the-art, media-rich interactive e-book that teaches teens and tweens about the dangers of purchasing counterfeit goods.

On June 8, 2021, the USPTO’s Patent Policy Team participated in the Hispanic National Bar Association (HNBA)-Microsoft IP Law Institute (IPLI), an annual IP program for law school students that provides an in-depth look into various career opportunities in the field of protection and enforcement of IP.

On June 30, 2021, the USPTO’s OPIA enforcement team, together with U.S. Customs and Border Protection, co-hosted the virtual workshop on *Beyond Registration: Taking Your Copyright and Trademark Rights to the Next Level*.

In celebration of the annual World Intellectual Property Day (April 26, 2021), USPTO headquarters and IP Attachés in cooperation with WIPO, other U.S. government agencies, and national IP offices hosted a number of events overseas in FY 2021 to commemorate and raise awareness of the 2021 global theme: *IP and SMEs: Taking Your Ideas to Market*. Events included a World IP Day flagship event encouraging U.S. SMEs to leverage IP to bring big ideas to market, which reached over 575 people, a related U.S. small business-focused World IP Day program conducted in cooperation with the Department of State, the Department of Commerce’s International Trade Administration, and the U.S. Copyright Office, as well as multiple events conducted in cooperation with U.S. Customs and Border Protection and the Small Business Administration.

Capacity-Building and Training

The USPTO's Global Intellectual Property Academy (GIPA)

In FY 2021, the USPTO's GIPA continued to develop and provide capacity-building programs, organized and conducted by OPIA attorneys, to help improve IP systems in key countries and regions to the benefit of U.S. stakeholders. Although traditional, face-to-face training programs did not take place during FY 2021, the USPTO continued to meet training obligations during this unprecedented time through increasing its leverage of various technologies to provide live online IP training. GIPA's established capacity for e-learning supported a successful pivot to all-remote delivery of its programs in mid-FY 2020 and continued this delivery in FY 2021. This included developing the technological capability to run virtual international meetings with simultaneous interpretation. Through these well-attended and well-received distance learning initiatives, the USPTO provided tailored content to developed and developing countries and Least Developed Countries (LDCs).

The programs addressed a full range of IP protection and enforcement matters, including enforcement of IP rights at national borders, Internet piracy, IP infringement involving expedited mail deliveries, trade secrets, copyright policy, and patent and trademark examination. Participants included officials with IP-related responsibilities, such as judges, prosecutors, patent and trademark examiners, and IP office administrators. In FY 2021, GIPA conducted 248 IP programs covering all areas of IP. About 78% of these programs targeted foreign officials with IP portfolios, engaging over 9,990 officials from 124 countries and intergovernmental organizations. A complete list of all countries represented at GIPA trainings in FY 2021 is available online at the USPTO Data Visualization Center (<https://www.uspto.gov/dashboards/externalaffairs/main.dashxml>). Generally, programs are delivered from GIPA's headquarters in Alexandria, VA, and around the world, through face-to-face and Distance Learning modes.

In the interest of further ensuring efficiency and coordination, GIPA also presented programs for U.S. officials and policymakers, providing updates on domestic and IP law and policy. The USPTO's OPIA once again collaborated with the Department of State's Foreign Service Institute (FSI) and Economic Bureau to provide (virtual) IP training for outbound Foreign Service Officers, and to provide subject matter expertise in developing an update to FSI's IP distance learning products. GIPA continues to improve its monitoring and evaluation capabilities, and implemented an updated logic model and multi-part survey in FY 2021. GIPA continued to engage in interagency training coordination meetings with other USG IP training donors such as DOJ, CBP, and DOC's CLDP program, on a whole-of-government basis as well as in smaller, more focused groups. These meetings facilitate discussions around avoiding duplication of efforts to allow agencies with aligned goals to leverage each other's resources to streamline the planning, execution and wrap-up of IP capacity building programs.

Other USPTO Activities Related to IP Protection and Enforcement

On January 24, 2020, the Department of Homeland Security (DHS) issued a report on *Combating Trafficking in Counterfeit and Pirated Goods*. The USPTO, in its role implementing aspects of the report, published *Federal Register* Notices on November 13, 2020, and January 11, 2021, to obtain comments from the public on two of the action items in the report: (1) Assess Contributory Trademark Infringement Liability for Platforms and (2) Establish a National Consumer Awareness Program. In August 2021, the USPTO published a paper summarizing the public comments on the November 13th *Federal Register* Notice.

In April 2021, pursuant to a Joint Project Agreement (JPA), USPTO and the National Association of Attorneys General (NAAG) Consumer Protection Training and Research Institute, co-organized an online roundtable briefing on the *Safety of Children's Products: Baby Food, Booster Seats, and Counterfeits* for State Attorney General (AG) Officers, attended by more than 150 State AG officers from across the country.

Africa

On March 8, 2021, USPTO's OPIA copyright team presented on the *Rights Implicated and Money Flow for Digital Uses of Copyrighted Music and Recordings* for member countries of the African Regional Intellectual Property Organization (ARIPO). Understanding the various rights implicated by the different digital uses will enable enforcement when those rights are not obtained.

On April 1, 2021, the USPTO's OPIA enforcement team participated in the International Trademark Association (INTA) webinar on *Local Initiatives, Coordination of Cross-Border IP Enforcement Measures, and International Support Measures Available in Africa*.

On May 6, 2021, the USPTO OPIA's enforcement team, in collaboration with the DOJ International Computer Hacking and Intellectual Property (ICHIP) advisor in Nigeria, provided training for 29 judges as part of ARIPO's event on *Enforcement Training for Judicial Instructors*.

In Winter, Spring and Summer 2021, under a Memorandum of Understanding (MOU) renewed in December 2020, the USPTO's OPIA Africa team developed and led a series of webinars with ARIPO for member states and observers, which collectively reached over 300 participants, on the topics of customs enforcement, trade secrets, enforcement (2 programs), geographical indications (2 programs), trademarks (2 programs), copyright (2 programs, including the above mentioned), patents, and fostering technology transfer in Africa, including a presentation on the success of the U.S. federal technology transfer system and the Bayh-Dole Act.

USPTO's Africa Team contributed to the planning of the ICHIP Nigeria's programming which sought to increase awareness in Africa about counterfeit vaccines and personal protective equipment (PPE).

USPTO's Africa Team provided training to the U.S. Foreign Commercial Service and State Department economic officers in Africa on IP issues, including enforcement. USPTO's OPIA also discussed proposed copyright law changes with the Governments of South Africa and Namibia.

Eurasia

In October and November 2020, USPTO delivered the content for a four-part webinar, organized with CLDP, for the National Intellectual Property Office of Georgia (Sakpatenti). USPTO provided the subject matter experts from OPIA (trade secrets), the USPTO Trademark Trial and Appeal Board (function of TTAB), Patent Trial and Appeal Board (function of PTAB) and the Office of the Chief Administrative Officer (teleworking).

In December 2020, USPTO's OPIA copyright team, together with its IP Attaché in Kyiv and the U.S. Copyright Office, provided technical assistance to Ukraine's Ministry of Economic Development and Trade on notice-and-takedown provisions in a draft law prepared by the Ministry.

In January 2021, OPIA presented on IP enforcement in the United States at the second meeting and workshop of the U.S.-Central Asia Trade and Investment Framework Agreement (TIFA) IP Working Group, organized by CLDP. OPIA coordinated content with USTR, CBP, IPR Center, and the IP Attaché in Kyiv. OPIA also participated in a Working Group meeting in July 2021.

In May 2021, OPIA held a preliminary dialogue on customs procedures and IP border enforcement with Ukrainian Customs officials from the Odesa region and the IP Attaché in Kyiv.

In June 2021 and September 2021, OPIA, with support from CBP, delivered two virtual workshops for Uzbekistan government officials on intellectual property enforcement at the border.

In July 2021, OPIA, with support from CBP, delivered a virtual workshop for Uzbekistan government officials on intellectual property enforcement at the border, focusing on risk targeting.

Latin America and Caribbean

Throughout the year, the USPTO IP Attaché office in Lima, Peru presented at 14 in-person and virtual training programs run by the Government of Peru and a law firm representing major brands. These programs trained more than 1200 officials all around Peru on the importance of combatting counterfeiting and provided practical advice from major stakeholders about how to identify counterfeits.

In October 2020, the USPTO and Peru's Judiciary signed an MOU to expand USPTO trainings on civil and criminal intellectual property law.

On October 16, 2020, the IP Advisor in the Brazil USPTO IP Attaché's Office joined a meeting of the Brazilian Bar Association – State of Rio de Janeiro (OAB-RJ) Commission of Piracy Studies and Combat during which upcoming actions and events by the Commission were discussed.

On October 22, 2020, the USPTO and the Brazil USPTO IP Attaché's Office participated in and supported a webinar on *Delivering Justice for IP Disputes During Covid-19* organized by the Brazilian Judiciary. The goal of the webinar was to share the unique perspectives and experiences of judges from Brazil, the U.S. and U.K. with delivering justice remotely during the COVID-19 pandemic, as well as to share reflections on the opportunities and challenges for courts in continuing to adapt to new circumstances in the future.

On October 27, 2020, the USPTO and the Brazil USPTO IP Attaché's Office participated in and supported a webinar on *Contemporary Aspects of Intellectual Property* organized by the School of Judges of the State of Rio de Janeiro (EMERJ). The program provided an opportunity for Brazilian Judges to engage in a dialogue with their American counterparts on preliminary injunctions in IP infringement actions, expert reports, opinions and testimony in IP cases, and the impact of precedent.

On November 2 & 4, 2020, the USPTO and the Peru IP Attaché's Office organized and participated in a two-day virtual seminar on *Trade Secret Protection and Enforcement* for approximately 100 Chilean IP officials covering the distinction between patent and trade secret protection, the elements of trade secret protection, the U.S. Government's approach to protecting trade secrets under the Defending Trade Secrets Act (DTSA) and the Economic Espionage Act (EEA), and trade secret challenges for small and medium enterprises.

On November 10, 2020, the USPTO IP Counselor in Mexico City and the OPIA trademark team conducted a webinar on *Likelihood of Confusion and Well-known Marks* for Dominican Republic government officials, including personnel from the Attorney General's Office.

On December 3, 2020, the USPTO and the Brazil USPTO IP Attaché's Office participated in a signing ceremony of the USPTO-Brazilian National Council to Combat Piracy (CNCP) MOU, which includes joint events, exchange of information, and public awareness activities.

On December 8-9, 2020, the USPTO's OPIA copyright team, joined by officials from the U.S. Copyright Office, participated in an *Online Seminar on Fighting Piracy in the Digital Environment* to discuss the U.S. experience protecting digital content. The program was organized by Mexico's Institute for Intellectual Property (IMPI) and Economia.

On February 2 and 4, 2021, the USPTO IP Counselor in Mexico City and the OPIA Enforcement team organized a two-day workshop in Mexico on civil and criminal trade secret protection for approximately 40 Officials from IMPI and SEPI (Sala Especializada en Materia de Propiedad Intelectual).

On February 8, 2021, the USPTO IP Counselor in Mexico City conducted a webinar to exchange best practices between customs authorities in Costa Rica and Mexico, in particular highlighting Mexico's Customs Trademark Database.

On May 3-4, 2021, the USPTO IP Counselor in Mexico City, in coordination with the DOJ ICHIP and OPIA Enforcement team, organized a two-day workshop on *Combating the Distribution of Counterfeit Medicines and Covid-19 Vaccinations* for approximately 150 customs, police, prosecutors, health regulations and IP Office officials from Guatemala, Honduras, El Salvador, Mexico, Suriname, Ecuador, Peru, and the Dominican Republic.

In order to assist the Dominican Republic (DR) Attorney General with its new IP Unit, the USPTO IP Counselor in Mexico City, the U.S. Embassy Santo Domingo, the DOJ ICHIP, OPIA Enforcement team, and the USPTO IP Attaché's Offices in Peru and Brazil collaborated on three roundtable discussions for the DR: with the National IP Coordination Center, Peru's CLCDAP (Comisión de Lucha Contra los Delitos Aduaneros y La Piratería) and Paraguay's CODEPI (National Center for the Defense of Intellectual Property Rights). The first discussion with the DR and the IPR Center occurred on March 19, 2021; the second discussion with Paraguay's CODEPI took place on May 2, 2021; and the last meeting with Peru's CLCDAP occurred on June 17, 2021.

On March 11, 2021, the USPTO IP Counselor in Mexico City conducted a webinar on Mexico's Piracy Study in cooperation with the International Trademark Association (INTA).

On July 8, 2021, the Brazilian Ministry of Justice and Civil Police in 9 different states, supported by the U.S. and U.K. Embassies, launched the third phase of "Operação 404" against digital piracy. Throughout Brazil, 334 websites and 94 streaming apps were blocked and suspended, including the removal of profiles on social media. "Operação 404" is considered by many (including U.S. stakeholders) to be an international model in the fight against digital piracy.

On August 3, 2021, USPTO participated in the IPR Center's *Intellectual Property Rights & Global Trade Enforcement Training* for Caribbean customs, police, and prosecutors by speaking remotely on the USPTO resources that are available to law enforcement (highlighting USPTO's interagency partnerships and collaboration on recent workshops) and the benefits of strong enforcement and statutory damages.

On August 19, 2021, the USPTO IP Counselor's Office in Mexico City participated in a training on counterfeit pharmaceuticals for GOM Officials, organized by the University of the Hemispheres in Quito and the Pharmaceutical Security Institute.

On September 8 and 9, 2021, the USPTO IP Counselor in Mexico City conducted a two-day virtual Judicial Colloquium for approximately 150 Judges from El Salvador, Honduras, Costa Rica, Guatemala, Mexico and the Dominican Republic on *Combating Intellectual Property Crimes*. Topics addressed during the colloquium included the application of civil and criminal remedies in copyright and trademark cases, provisional measures, evidentiary issues in IP cases, requests for search warrants and seizure orders, and asset forfeiture and achieving deterrence for IP crimes.

On September 28- 29, 2021, the USPTO IP Counselor’s Office in Mexico City organized a two-day virtual workshop on *Best Practices for the Destruction of Forfeited IP Infringing Goods* for approximately 75 customs and IP office officials in the CARICOM countries. The workshop focused on chain of custody for suspected IP infringing goods; administrative and criminal forfeiture of IP infringing goods; best practices in the destruction and disposal of infringing goods; and an overview of the U.S. Forfeiture Fund to support IP investigations, the storage and destruction of infringing goods, and the disruption of criminal enterprises.

South East Asia

From September 2020 through March 2021, the IP Attaché for Southeast Asia, in cooperation with multiple stakeholders, including the Thai Department of Intellectual Property and rightsholders, organized a *Go for Real* video-clip contest and a series of four IP education webinars to address online intellectual property rights violations. A total of 94 video clips from 91 teams of three members were submitted for the contest, and several hundreds of students, academic staff, rightsholders, and the general public participated in the webinars. Three videos were recognized, and they are used to promote IP awareness on multiple online platforms and have been broadcast on numerous Thai television channels.

From September 17, 2020 through January 21, 2021, the USPTO’s OPIA patent and enforcement teams organized and participated in a series of 17 webinar sessions (15 of which occurred in FY 2021) on *Adapting Intellectual Property Laws to Promote Innovation and Creativity in New Technologies*, held in conjunction with the Intellectual Property Office of Singapore and jointly sponsored by the Singapore Cooperation Program and the U.S. Department of State under the Singapore-United States Third Country Training Programme (TCTP). The program explored the intersection of new, disruptive technologies and the role of governments in fostering those technologies, particularly with respect to intellectual property policies. Several sessions focused on enforcement-related issues faced by civil litigators, law enforcement authorities, criminal prosecutors, and the courts.

In October 2020, the IP Attaché for Southeast Asia discussed the protection and enforcement of plant-related intellectual property in the United States at two programs organized by the Plant Variety Protection Office of Vietnam in Hanoi and Can Tho, Vietnam. Each program had over 100 Vietnamese participants.

In October 2020, the USPTO organized and moderated two panel sessions on enforcement as part of USPTO’s *APEC Virtual Workshop on Design Protection and Enforcement*, and organized and moderated an *APEC Webinar on Content Protection and Illicit Streaming: Enforcement Approaches and Strategies*. These were attended by several hundred government officials from throughout the region.

In October 2020, the USPTO and the U.S. Mission to ASEAN co-organized a webinar on *Copyright Protection and Enforcement in the Online Digital Environment* as part of the ASEAN Connect Digital Economy series. The event was attended by several hundred government officials from throughout the region.

In December 2020, the USPTO organized and conducted a nine-part webinar roundtable series on *Intellectual Property Civil and Criminal Enforcement and Case Management* for judges from the Southeast Asia and South Pacific regions. The event was attended by more than 100 foreign judges and 11 U.S. judges.

In March 2021, the USPTO, in collaboration with the U.S. Mission to ASEAN, organized a webinar on copyright protection and enforcement in the online digital environment. Approximately 290 government officials, content creators, academics, and IP practitioners attended the program.

In March 2021, the USPTO IP Attaché for Southeast Asia – in cooperation with the Asian Law Students Association (ALSA) – organized an overview of IP protection, the U.S. legal systems for protecting plant-related inventions, and UPOV 1991 that was attended by approximately 117 law students from Indonesia, the Philippines, Thailand, and Vietnam. In June 2021, the USPTO IP Attaché, again in cooperation with ALSA, organized a two-day webinar on copyright protection and enforcement in the digital environment.

On March 22, 2021, the IP Attaché for Southeast Asia, the U.S. Embassy Jakarta, and the Directorate General of Intellectual Property of Indonesia (DGIP) co-organized a *Webinar on IPR Enforcement Coordination for Indonesia* to discuss IPR enforcement coordination with a total of 111 Indonesian authorities. Key presenters included representatives of the U.S. Homeland Security Investigations, the Thai Department of Intellectual Property, and the Intellectual Property Office of the Philippines (IPOP HL).

In May 2021, the IP Attaché for Southeast Asia facilitated the establishment of an MOU between the USPTO and IPOP HL that replaced a prior MOU and provides for continuing cooperation between the two offices on intellectual property matters, particularly in the areas of technical assistance, training, and capacity building.

On July 7, 2021, the IP Attaché for Southeast Asia Office virtually attended a public consultation on the draft amendment to the Copyright Act of Thailand hosted by the Parliament's Ad-hoc Committee.

On July 14, 2021, the IP Attaché for Southeast Asia Office and U.S. Embassy Jakarta co-organized a roundtable discussion on *Online Counterfeit Products and Medicines—Risks and Solutions* that addressed the counterfeit challenges and identified possible solutions for effectively combatting the online trade of illicit items, substandard healthcare, and consumer products in Indonesia. Approximately 153 participants from Indonesia government agencies, e-commerce platforms, and rightsholders attended the program.

On August 3, 2021, the IP Attaché for Southeast Asia participated in the 64th ASEAN Working Group on IP Cooperation. The meeting was hosted by the ASEAN Secretariat and representatives of ASEAN members' IP offices. The IP Attaché presented a list of proposed USPTO 2021-22 training programs to be conducted under the USPTO-ASEAN MOU.

On August 18-19, 2021, the IP Attaché for Southeast Asia and the OPIA Senior Counselor for Enforcement hosted the *ASEAN Workshop on Trade Secret Protection and Enforcement* in collaboration with the ASEAN Secretariat. The two-day workshop had approximately 130 participants/day, most of whom were officials from national IP offices and law enforcement agencies across ASEAN members, Papua New Guinea, and Timor Leste.

In September 2021, USPTO, in partnership with the Intellectual Property Office of Singapore, conducted a U.S.-Singapore Third Country Training Program (TCTP) online course on *Intellectual Property and the Digital Economy*, which included several sessions focusing on enforcement-related issues faced by civil litigators, law enforcement authorities, criminal prosecutors, and the courts. More than 100 people participated in the course.

On September 15, 2021, the IP Attaché for Southeast Asia Office and the U.S. Embassy Jakarta worked with the Government of Indonesia to discuss a potential MOU with rightsholders/e-commerce platforms to address online counterfeiting and piracy. Representatives of the Department of Intellectual Property of Thailand and the Intellectual Property Office of the Philippines also participated in the discussion to share their insights. Indonesian participants included 20 officials from Ministry of Trade, the Directorate General of Intellectual Property, the National Agency of Drug and Food Control, and Ministry of Communication and Information Technology.

The IP Attaché for Southeast Asia worked closely with U.S. stakeholders in protecting their IP in countries in the region. In addition to providing relevant advice and recent development on IP law and policy and raising their IP concerns with the respective local governments, the IP Attaché also participated in and provided insights on the following programs.

- **The International Anti-Corruption Conference Webinar, November 2020**

On November 17, 2020, the IP Attaché for Southeast Asia participated in the *IP Webinar on IP Status in South Asia and Southeast Asia* hosted by the International Anti-Counterfeiting Coalition (IACC). The IP Attaché discussed recent IP developments in the Southeast Asia region with approximately 76 representatives of IP stakeholders and brand-owners.

- **Virtual Southeast Asia IP Roadshow, March 2021**

On March 5, 2021, the IP Attaché for Southeast Asia participated in a webinar on *Protecting and Enforcing IPRs in Southeast Asia: What Small Businesses Need to Know* (or *SE Asia IP Roadshow*) organized by USPTO-OPIA in cooperation with the US-ASEAN Business Council, the U.S. Department of Commerce's International Trade Administration, and the U.S. Commercial Service. The webinar provided IP information, including experiences and practical challenges in doing business in Southeast Asia. The IP Attaché spoke on the USPTO- IP Attaché program and the services provided by the IP Attaché Southeast Asia Office. Over 200 business entrepreneurs, legal practitioners, and officials in the U.S. and the SEA region attended the program.

South Asia

On October 16, 2020, the IP Attaché for South Asia office collaborated with the Federation of Indian Chambers of Commerce and Industry (FICCI), on training for the police officers of Jammu & Kashmir on the prevention of counterfeiting and smuggling.

In November 2020 through January 2021, the USPTO South Asia IP Counselor's office hosted a series of virtual sessions on *Dark Web Investigation and Prosecution of IP crimes* for officials of the Maharashtra police, which have a dedicated unit for IP-related crimes known as the Maharashtra Cyber Digital Crime Unit (MCDCU). Officers from MCDCU actively participated in the sessions and inquired about how U.S. law enforcement can assist in obtaining information from U.S.-based Internet Service Providers (ISPs) regarding registered websites that host pirated copies of copyrighted content from India. Stemming from this effort, the Mumbai Crime Unit expressed interest in organizing more programs with USPTO to increase IP awareness and effective enforcement mechanisms for police, customs, and enforcement officials in Maharashtra.

On January 13, 2021, USPTO's OPIA copyright team presented on the *Rights Implicated and Money Flow for Digital Uses of Copyrighted Music and Recordings* for the Indian Joint Secretary of the Department for Promotion of Industry and Internal Trade (DPIIT). The presentation discussed the various rights that are implicated by different digital uses.

On February 9, 2021, the USPTO – in partnership with CLDP, USAID, FDA, CBP and other U.S. agencies – launched a multi-part series to exchange best practices on combating counterfeit medicines and medical devices with enforcement officials from the Government of Pakistan. This ongoing effort seeks to curb the flow of counterfeit pharmaceuticals into and out of Pakistan by enhancing the capacity of Pakistan customs officials to help protect the country's drug supply from the threat of counterfeits. Through the program's many sessions, participants received instruction on forensic tools to help identify counterfeit products, engaged in discussions on pharmaceutical supply chain integrity, heard directly from cyber intelligence experts, and learned ways to identify trends and patterns of transnational criminal organizations exploiting trade routes. This program will continue to build and strengthen the relationship between and among the participants, including the use of an interagency approach for addressing intellectual property rights enforcement issues and protecting public health and safety. Three of the four multi-session modules were delivered by the end of FY 2021. These sessions saw participation and representation by Pakistan's Intellectual Property Office, customs officials, and the Drug Regulatory Authority of Pakistan (DRAP), and were supplemented with real-world industry perspectives (local and multinationals).

In March 2021, the U.S. Intellectual Property Counselor for South Asia (also known as the IP Attaché for South Asia) received a message through the STOPFakes.Gov portal indicating substantial counterfeit activity in Mumbai, India involving hundreds of counterfeit sport jerseys and other apparel adorned with logos of various U.S. brands like Nike, Puma and Under Armor. After verifying the activity as a warehouse supplying the potentially illicit products to other vendors, both locally and through online sources, the USPTO's South Asia office coordinated

with an IP enforcement agency to review and subsequently act on the counterfeiting activity, with civil raids successfully conducted at the target source.

On July 8, 2021, the IP Counselor for South Asia provided opening remarks during an enforcement best practices session with the law enforcement and health ministries from the governments of Sri Lanka and the Maldives. The program, co-developed by Homeland Security Investigations (HSI) and Pfizer, was designed to raise awareness of how best to identify Pfizer's authentic COVID-19 vaccine products and ways they are being misrepresented or faked by infringers in the marketplace. HSI provided an overview of their operations, including Operation Stolen Promise, and the IP Counselor spoke about recent and ongoing IP and enforcement efforts with the Sri Lankan and Maldivian governments.

On August 28, 2021, the IP Counselor for South Asia delivered the keynote at the plenary session on the "Role of Intellectual Property in Inclusive Growth" at the 2021 Returning Mothers Conference organized by the Institute of Electrical and Electronics Engineers (IEEE) and the Madras Women in Engineering (WIE). The IP Counselor highlighted the importance of IP, IP awareness, anti-counterfeiting measures citing examples of counterfeit toys and baby products, and the need to raise the respect for IP. He also spoke about the USPTO study on women and innovation and efforts related thereto. The program drew more than 100 attendees.

On September 15, 2021, the USPTO South Asia office – in collaboration with Punjab State Council for Science & Technology and IISER, Mohali – organized an open knowledge session attended by 30 participants from start-up and research institutes. The IP Counselor spoke on IPR initiatives and the importance of strong IPR protection and enforcement. IP specialists spoke on the importance of patent quality, funding opportunities, and “Do’s and Don’ts” for startups. The session was attended by 30 participants from start-up and research institutes.

Middle East/North Africa

On November 20, 2020, USPTO – in partnership with CBP's IPR Branch and National Threat Analysis Center – conducted an IPR Border Enforcement Workshop for Jordan and Moroccan Customs. The program hosted 25-30 participants and was positively received.

From December 7-10, 2020, USPTO conducted a multi-day virtual workshop on IP piracy for Saudi Arabia, Kuwait, and Jordan that leveraged USG interagency support including the FCC, DOJ CCIPS, and HSI. The program hosted between 70-80 participants and underlined the need for law enforcement to build out relationships with third parties involved with the facilitation of online piracy (such as website hosting services, internet service providers and proxy servers). It included an exchange with industry representatives and active engagement with focused questions and comments.

On September 2, 2021, USPTO held a two-hour IP Enforcement discussion with several Algerian government ministries, including Ministry of Justice, ONDA (Copyright Office), IP office, Ministry of Commerce, and Police. The discussion included updates from previous consultations, and the officials identified specific needs for technical assistance and capacity building, which will be incorporated into future virtual and in-person engagements.

East Asia

In FY 2021, the Shanghai IP Attaché's office provided commercial assistance on numerous IP matters related to food, beverage, infant care, architecture, kitchen appliance, renewable energy, pharmaceuticals, medical device, biotech, personal protective equipment, personal care, information and communications technology, and financial services industries.

In November 2020, the Senior IPR Specialist for the Shanghai IP Attaché's office was given the Mission Honor Award for team collaboration at post in assisting U.S. auto parts manufacturers to better prepare for the challenges and opportunities they face in China's automotive aftermarket.

In November 2020, the Shanghai IP Attaché's office facilitated USG participation in the *Forum on International Cooperation in Fighting against IPR Infringement and Counterfeiting* organized by the Ministry of Commerce at the China International Import Expo. On the margins, the Intellectual Property Counselor in Beijing met with major U.S. rightsholders.

In February-March 2021, the USPTO's OPIA China Team hosted a two-part webinar series on *IP Protection and Enforcement Basics in China*, providing U.S. businesses, inventors, and intellectual property (IP) rightsholders doing business in China the opportunity to hear from senior USPTO attorneys and guest practitioners about protection and enforcement of all categories of IP in China. The webinar had hundreds of attendees.

In June 2021, the USPTO's OPIA China Team launched a quarterly update series on legislation and case law in China. At the June webinar update, the OPIA China Team covered nearly one and a half years of legal changes in China in all areas of IP protection and enforcement. The update provided U.S. businesses, inventors, and IP rightsholders the opportunity to hear from senior USPTO attorneys about the recent developments, and obtain the knowledge needed to navigate China's rapidly changing IP landscape. In September 2021, the China Team hosted a second update, on IP developments in China during the previous quarter. Each webinar had hundreds of attendees.

In May 2021, the Shanghai IP Attaché's office hosted IP-themed outreach to Chinese counterparts at the Shanghai Intellectual Property Administration, the Shanghai High Court/Shanghai IP Court, and the Zhejiang IPO. The office also facilitated meetings with the IP Counselor in Beijing and U.S. stakeholders including AmCham Shanghai and its 40-plus members and the U.S.-China Business Council and its members.

In July 2021, the USPTO's OPIA China Team hosted a webinar on China IP for U.S. government officials. The IP Counselor in Beijing provided a "view from the ground" perspective on China's IP landscape, and the webinar included an overview of recent issues and legal changes that U.S. rightsholders are most likely to encounter in the areas of trademarks, copyrights, patents, and enforcement.

European Union

During FY 2021, the Brussels-based USPTO Attaché for Europe (USPTO Brussels) continued to engage with counterparts in the EU institutions and key EU Member States to facilitate the sharing of best practices on IP enforcement; explore areas of transatlantic cooperation, such as sharing of customs data to enhance enforcement efforts; and plan public-awareness and capacity-building programs and campaigns. With respect to China's detrimental influence in IP matters relevant to U.S. stakeholders and EU economies (especially the sustained surge of China-origin counterfeit and substandard COVID-19 related products), the Brussels team continued to emphasize the importance of establishing a strong risk-based, national-security-focused customs screening system that identifies and removes counterfeit goods from the stream of commerce.

USPTO Brussels continued its work in raising public awareness of the importance of IP protection and enforcement, especially as it relates to consumer health and safety, including the situation around the COVID-19 crisis and ensuing economic recovery efforts. To that end, the Attaché spoke at the European Parliament program related to consumer protection against unsafe products bought online. The Brussels team also again marked World Anti-Counterfeiting Day on social media, emphasizing the critical importance of stopping counterfeits in the marketplace.

Oceania

In June 2021, the USPTO presented on a panel session of a Criminal Business Disruption Workshop, organized by the Oceania Customs Organization Secretariat for its member territories and customs authorities.

DEPARTMENT OF DEFENSE

DEPARTMENT OF DEFENSE

Department of Defense Appendix for FY 2021 Annual Report

This appendix discusses the FY 2021 activities of the Department of Defense (DoD).

DoDI 5000.90: On December 31, 2020, the Office of the Under Secretary of Defense for Acquisition and Sustainment published DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers. This issuance establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk by program decision authorities and program managers (PMs) in the DoD acquisition processes. Over the past decade, the United States' strategic competitors have been able to exploit vulnerabilities in the DoD supply chain by stealing U.S. intellectual property and decreasing confidence in the security of products delivered to the DoD. Contractor facilities—including design, development, and production environments, networks, supply chains, and personnel— can be used by threat actors as cyber pathways to access government program organizations or fielded systems to steal, alter, or destroy system functionality, information, or technology. Program Managers conduct Supply Chain Risk Management (SCRM) to include Cyber-SCRM. This includes conducting market research to assess potential vendors to determine if they:

(1) Provide products and components, or sub-components, sourced through original equipment manufacturers or authorized resellers.

(2) Have previously incurred significant malicious network intrusions, data breaches, and loss of client data or intellectual property.

(3) Have obtained a Cybersecurity Maturity Model Certification (CMMC) level indicating that they practice, at least, basic cyber hygiene (e.g., access management, timely patch management, identity management, and password management).

The Protecting Critical Technology Task Force: The Secretary of Defense established the Protecting Critical Technology Task Force (PCTTF) in 2018 to protect U.S. critical technologies wherever they reside, regardless of how they are being taken, using every tool and authority at their disposal.

During FY 2021, the Task Force integrated the activities of multiple organizations, accelerated the pace, and scaled technology-protection best practices across the Department. It was the Task Force's job to identify and remove roadblocks, shrink timelines for implementation, facilitate senior decision-making, advocate for resources, and drive the Department to better address the technology transfer problem. The Task Force worked across four Lines of Effort (LOEs):

(1) Protect the Defense Industrial Base (DIB);

(2) Protect the Research and Development Enterprise;

(3) Block Malicious Foreign Investment and Acquisition; and

(4) Disrupt and Deny Threat Actors.

Within these four LOEs, the Task Force established ten primary objectives:

1. Develop and Operationalize the Critical Programs and Technology (CP&T) List to drive DoD protection (OUSD R&E);
2. Increase cybersecurity in the DIB (OUSD A&S);
3. Integrate security into the requirements and acquisitions process (OUSD I&S);
4. Prevent individuals with problematic foreign influence from working on DoD-funded research (OUSD R&E);
5. Counter adversary talent recruitment programs (OUSD R&E);
6. Prevent adversaries from acquiring our critical and emerging technologies through acquisition and investment (OUSD A&S);
7. Expand protection of DoD critical technologies via export controls (OUSD A&S);
8. Undermine adversary confidence in exfiltrated data (OUSD I&S);
9. Operationally respond to cyber threat actors targeting the DIB (OUSD I&S); and
10. Expose Chinese and Russian theft of critical technologies (All).

The 2020 DoD CP&T List is the single, authoritative Department list for which protection resources should be applied in accordance with law, regulations, and government-wide policies. This CP&T effort is driven from FY 2019 NDAA, Section 1049 – “The Secretary of Defense shall establish and maintain a list of acquisition programs, technologies, manufacturing capabilities, and research areas critical for maintaining the national security technological advantage of the United States over foreign countries of special concern.” The revalidation of the CP&T List will continue to be a DoD annual congressional requirement, led by the Office of the Under Secretary of Defense, Research & Engineering.

As a short duration task force, the PCTTF sunsetted in June 2021. Going forward, the appropriate OSD component(s) assigned to each primary objective listed above will continue to coordinate DoD’s efforts for those mission areas and activities.

Cybersecurity Maturity Model Certification (CMMC): In accordance with FY 2020 NDAA Section 1648, the Department developed a risk-based cybersecurity framework to enhance the protection of Federal Contract Information and CUI in the DIB sector. In order to implement this framework, the Department published DFARS interim rule 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements, in the *Federal Register* at 85 FR 61505, and effective on November 30, 2020. The Department is currently undertaking an

internal review regarding CMMC implementation. The drafting team continues to review public comments received in response to the interim DFARS rule.

Defense Acquisition University: The Defense Acquisition University (DAU) engaged in several educational initiatives during FY 2021 that reflect the following themes:

- (1) the critical role intellectual property plays in maintaining military technological superiority in emerging technologies (e.g., big data analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, biotechnology);
- (2) DoD's desire to assist U.S. Government agencies to identify and build partnerships to address areas of economic, technological, and informational vulnerabilities; and
- (3) the need to respect and protect technology development investments by both the private sector and U.S. Government from intellectual property theft by both domestic and foreign actors.

FY 2021 DAU Educational Initiatives

- Developed a five-year Strategic Plan for DAU's intellectual property (IP) program, focusing on creating educational resources on IP to maintain U.S. technological superiority and building partnerships with U.S. Government agencies (e.g., IP, trade, enforcement, intelligence), industry (large and small businesses), academia, associations, and consortia.
- Established a website (intellectual property Community of Practice) as a one-stop shop for the dissemination of IP training resources, policy and legislation, best practices, and other resources.
- Created seven targeted on-demand videos on IP topics important to the acquisition of defense technologies.
- Reviewed DAU online IP modules for a comprehensive revamp focused on scenario exercises, interactive tools and interfaces, and enhanced graphics.
- Conducted live and virtual workshops with DoD and industry representatives on key IP topics (e.g., pricing/IP valuation and evaluation) and IP workshops for engineering staff.

Naval Criminal Investigative Service (NCIS)

The Naval Criminal Investigative Service Safeguards Department of the Navy (DON) acquisition programs and protects the DON's capital investments in technology by conducting investigations and operations that reduce product substitution, combat corruption, and disrupt foreign exploitation of DON acquisition. Reducing product substitution remains a top priority for NCIS to ensure the DON procures products that meet safety standards for the warfighter, thereby enhancing operational readiness and lethality.

As competitors of the United States continue to modernize their militaries, the advantage of early detection of counterfeit goods has become increasingly clear. Early detection mitigates degraded platform capabilities and improves battlefield reliability and superiority. To proactively combat the threat posed by counterfeit goods, NCIS is a partner in Operation Chain Reaction, which is led by the National Intellectual Property Rights Coordination Center and targets counterfeit goods entering the supply chains of the Department of Defense and other U.S. Government agencies. Through extensive partnerships, NCIS has successfully reduced this threat to the warfighter.

Additionally, a joint investigation involving NCIS led to the indictment of a defense contractor in 2020 for selling Chinese-made body armor and other related goods to Federal agencies, including the DON. The investigation determined that the contractor falsely certified that the ballistic vests, helmets, riot gear, and other items he offered for sale were manufactured in Hong Kong and the United States when, in fact, they were manufactured in China, in violation of U.S. law. NCIS participated in the joint investigation with the GSA Office of Inspector General; the State Department Office of Inspector General; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Army Major Procurement Fraud Unit; the Defense Criminal Investigative Service; HSI; the FBI; the Air Force Office of Special Investigations; the Coast Guard Investigative Service; and the U.S. Attorney's Office for the District of Maryland. The DOJ press release is at <https://www.justice.gov/usao-md/pr/virginia-defense-contractor-pleads-guilty-federal-charges-maryland-illegally-selling>.

**DEPARTMENT OF HEALTH AND HUMAN
SERVICES**

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration (FDA) Appendix for FY 2021 Annual Report

This appendix discusses the FY 2021 activities of the Food and Drug Administration (FDA).

Drug counterfeiting and adulteration are serious threats to public health. Counterfeit or unapproved drugs raise significant public health concerns because their safety and effectiveness are unknown. In the United States, a relatively comprehensive system of laws, regulations, and enforcement by Federal and state authorities have helped reduce drug counterfeiting incidents, and FDA works to ensure that Americans can have a high degree of confidence in the approved drugs that they obtain through legal channels. FDA has made it a priority to investigate reports of counterfeit and unapproved drugs and works with U.S. drug supply chain stakeholders to improve our ability to prevent, detect, and respond to threats of counterfeit, unapproved, and substandard drugs. FDA also educates consumers and the health care community about the risks of, and minimizing exposure to, counterfeit, unapproved, and substandard drug products through oversight of voluntary recalls, public awareness campaigns, and other steps. Additionally, FDA reaches beyond U.S. borders and works with our foreign counterparts to identify global supply chain vulnerabilities as well as identify and implement realistic solutions, nationally and internationally.

Improving the Security of the Pharmaceutical Supply Chain

Drug Traceability

FDA continues to implement provisions of the Drug Supply Chain Security Act (DSCSA) (Title II of the Drug Quality and Security Act) that was enacted on November 27, 2013. The DSCSA helps to improve the integrity and security of the pharmaceutical distribution supply chain for most prescription drugs by establishing product tracing, product identifier, authorized trading partner, and verification requirements for manufacturers, repackagers, wholesale distributors, and dispensers. The DSCSA also requires critical steps to build an electronic, interoperable system to identify and trace such prescription drugs that are distributed in the United States by 2023, in addition to development of national standards for licensure of wholesale distributors and third-party logistics providers. Among other actions to help secure the supply chain, the DSCSA is intended to facilitate the exchange of information to verify product legitimacy, enhance detection and notification of an illegitimate product, and facilitate product recalls.

In FY 2021, FDA issued several key guidance documents for industry. In October 2020, FDA issued compliance policies to minimize possible disruptions in the distribution of certain prescription drugs in the U.S. because some wholesale distributors expressed a need for additional time beyond November 27, 2020, before they can begin verifying returned products prior to resale or other further distribution in an efficient, secure, and timely manner. Also, some dispensers (primarily pharmacies) also needed additional time to perform certain verification activities in investigating suspect product or when responding to a notification of illegitimate product from FDA or another trading partner. Under these compliance policies, FDA does not

intend to take action before November 27, 2023, against wholesale distributors or dispensers who do not comply with these verification requirements. Trading partners can use the additional time to ensure the systems and processes that are put into place meet the enhanced system requirements by November 27, 2023.

In June 2021, FDA finalized two guidance documents and published two draft guidance documents regarding DSCSA requirements that prescription drugs be identified and traced properly as they move through the supply chain. These guidance documents lay out the FDA's recommendations for how to comply with applicable DSCSA requirements, including those for enhanced drug distribution security at the package level that go into effect in November 2023. The guidance documents are summarized below:

- The final guidance on *Product Identifiers Under the Drug Supply Chain Security Act, Questions and Answers* addresses the DSCSA requirement that manufacturers and repackagers affix a product identifier on drug packages. This includes the product's national drug code (NDC), serial number, lot number and expiration date on each package and homogenous case of product, in human- and machine-readable form. The machine-readable form is generally a two-dimensional data matrix barcode. Possible industry questions are clarified in the final guidance.
- The final guidance on *Drug Supply Chain Security Act Implementation: Identification of Suspect Product and Notification* is intended to aid certain trading partners in identifying a suspect product and specific scenarios that could significantly increase the risk of a suspect product entering the pharmaceutical distribution supply chain. The guidance document also describes how trading partners should notify the FDA of illegitimate product and sets forth a process for terminating notifications of illegitimate product in consultation with the FDA. In addition, this guidance document responds to comments from stakeholders to clarify certain points and finalizes the remaining draft portion, i.e., describing when manufacturers should notify the FDA of a high risk that a product is illegitimate, of the otherwise final guidance issued in December 2016.
- When finalized, the revised draft guidance on *Definitions of Suspect Product and Illegitimate Product for Verification Obligation under DSCSA* will lay out the FDA's thoughts on terms used to define "suspect" and "illegitimate" products, to help trading partners determine when to report an illegitimate product to FDA under the DSCSA's verification requirements. These terms include "counterfeit," "diverted," "stolen," "fraudulent transaction," and "unfit for distribution." In response to comments received from stakeholders, this draft guidance revises the March 2018 draft guidance.
- The draft guidance on *Enhanced Drug Distribution Security at the Package Level under DSCSA* is intended to assist supply chain stakeholders, particularly trading partners, with requirements for enhanced drug distribution security at the package level that go into effect on November 27, 2023. When finalized, this guidance will provide recommendations on the system attributes necessary for enabling the secure tracing of product and verification at the package level.

FDA is planning for additional stakeholder engagement and discussions on systems and processes needed for enhanced supply chain security requirements that go into effect in 2023. For updates about DSCSA implementation and copies of the guidance documents see <http://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/default.htm>.

Engagement with Other Countries

Asia Pacific Economic Cooperation (APEC) Global Medical Product Quality and Supply Chain Security Efforts

FDA is the global lead for the APEC Supply Chain Security Toolkit, which is a comprehensive resource that addresses prevention, detection, and response with regards to vulnerabilities in the medical product supply chain. It covers the entire supply chain and life cycle of medical products. The toolkit is the culmination of a collaborative project that was commissioned by APEC with the oversight of the Life Sciences Innovation Forum (LSIF) and the Regulatory Harmonisation Steering Committee.

In February 2021, FDA presented the toolkit to the Subcommittee on Customs Procedures (SCCP) and the LSIF meetings at the First Senior Officials' Meetings (SOM1) which were led and hosted by New Zealand's Ministry of Health. Additionally, this Priority Work Area (PWA) Champion is currently updating the supply chain toolkit particularly on internal sales and post-marketing surveillance due to the feedback from pharmaceutical industry, member states regulators, United States Pharmacopeia (USP), and World Health Organization (WHO).

Furthermore, APEC endorsed a new Center of Excellence (COE) for Taylor's University of Malaysia in January of 2020 that collaborated with USP in co-hosting several workshops for which FDA gave guidance as the PWA lead. As part of this effort, in March 2021, FDA participated virtually in a meeting convened by the USP and Taylor's University COE for Global Supply Chain Integrity in collaboration with the APEC LSIF and Ministry of Health Malaysia. This included a series of webinars culminating in a two-day training session on global supply chain integrity. The onset of the COVID-19 pandemic and the arrival of COVID-19 vaccines highlight the importance of fortifying vulnerable medical supply chains with a proper understanding of traceability and distribution of medical products. FDA presented on topics including good distribution practices and track-and-trace, and highlighted the utility of the toolkit in preventing, detecting, and responding to breaches in the medical product supply chain.

WHO Member State Mechanism

FDA is highly involved in the technical, policy, and strategic implementation of the World Health Organization Member State Mechanism on Substandard and Falsified Medical Products (WHO MECH) and serves as a vice-chair for the America's region on its Steering Committee. FDA supports the WHO MECH in its global efforts to prevent, detect, and respond to substandard and falsified (SF) medical products, including the development of reports, guidance, tools, and other products. The WHO MECH, composed of public health and national

medicines regulatory authorities, focuses on the public health aspects of SF medical products, and does not address intellectual property rights issues.

Global Surveillance and Monitoring System

FDA has supported the World Health Organization (WHO) to establish the Global Surveillance and Monitoring System (GSMS) for Substandard and Falsified Medical Products which was launched in 2013. The GSMS provides national medicines regulatory authorities (NMRAs) with an information portal to report counterfeit medical products, and the ability to check if similar products have been found around the globe. If similar products have been found, the WHO works with NMRAs to investigate suspected counterfeit cases and issue alerts as necessary. The GSMS portal is available in English, French, Spanish, and Portuguese. The online portal, search facility, and access to the photo library have also enhanced participation by Member States. Manufacturers can also submit information on counterfeit products to the GSMS. The WHO has reported that the quality and number of reports to GSMS has been steadily increasing in the last few years.

Illegal Opioids and Other Consumer Education

Illegal Opioids Online and Warning Letters Issued

Opioid addiction is an immense public health crisis and addressing it is one of FDA's highest priorities. Tragically, more than 100,000 Americans have died from drug overdoses in the 12 months leading up to April 2021, representing a 28% increase over the same period last year.³ The illegal online marketing of unapproved opioids is particularly concerning in light of the nation's opioid addiction and overdose epidemic. In addition, opioids bought online may be counterfeit and could contain other dangerous substances.

During FY 2021, FDA issued four warning letters to the owner(s)/operator(s) of internet pharmacy websites illegally offering for sale unapproved and misbranded opioids to U.S. consumers.

Unproven products that claim to treat or prevent COVID-19 and other conditions

As part of its response to the public health emergency, FDA has also addressed the increase in unproven products sold with fraudulent COVID-19 claims and has issued more than 180 warning letters to companies. See <https://www.fda.gov/consumers/health-fraud-scams/fraudulent-coronavirus-disease-2019-covid-19-products> for more information. In addition, since the start of the COVID-19 pandemic, FDA has issued 17 warning letters to owners and/or operators of internet pharmacy websites that illegally offer for sale unapproved and misbranded drugs purported to treat COVID-19 to U.S. consumers. See <https://www.fda.gov/drugs/drug-supply-chain-integrity/internet-pharmacy-warning-letters>. FDA issued 84 health fraud public

³ FACT SHEET: The Biden Administration Launches New Efforts to Counter Transnational Criminal Organizations and Illicit Drugs, December 15, 2021 *available at:* <https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/15/fact-sheet-the-biden-administration-launches-new-efforts-to-counter-transnational-criminal-organizations-and-illicit-drugs/>

notifications in FY21. See <https://www.fda.gov/consumers/health-fraud-scams/public-notifications-and-safety-alerts-health-fraud>.

The FDA's Operation Quack Hack leveraged agency expertise and advanced analytics to protect consumers from fraudulent medical products during the COVID-19 pandemic. Building upon our previous experience with illegal online pharmacies, a team of consumer safety officers, special agents, and intelligence analysts triage incoming complaints about fraudulent and unproven medical products. Where appropriate, complaints are sent to other agencies or to FDA centers for additional review and possible follow-up action. In some cases, following a preliminary investigation, the Operation Quack Hack team sends an abuse complaint to the domain name registrars or a report to online marketplaces. As of September 30, 2021, FDA issued more than 600 abuse complaints and reports, which are intended to notify companies that may not have been aware that their platforms were being used to sell an unapproved, unauthorized, or uncleared medical product during the COVID-19 pandemic. Through Operation Quack Hack, online marketplaces and registrars have been notified by the FDA of more than 2,100 fraudulent COVID-19 related product listings and websites. Please see [FDA's website](#) for more information regarding Operation Quack Hack.

On December 27, 2021, the U.S. District Court for the District of New Jersey entered a consent decree of permanent injunction that prohibits a New Jersey-based company from receiving or distributing any drugs until the company complies with the Federal Food, Drug, and Cosmetic Act (FD&C Act) and other requirements. The complaint, filed by the Department of Justice on behalf of the FDA, alleged that Natural Solutions Foundation, an organization, and its two principals, Rima Laibow and Ralph Fucetola, violated the FD&C Act by selling unapproved and misbranded drugs intended to cure, mitigate, treat or prevent COVID-19. The defendants had received a jointly issued warning letter from FDA and FTC on May 19, 2020.

FDA Warns Consumers to Avoid Certain Male Enhancement and Weight Loss Products Sold Through Amazon, eBay, and Other Retailers

In December 2020, [FDA warned consumers](#) not to use nearly 50 sexual enhancement or weight loss products that have been found to contain hidden ingredients and may pose a significant health risk. FDA purchased 51 products from Amazon and eBay for testing, and 46 of the products tested were found to contain undeclared active pharmaceutical ingredients. The FDA's laboratory testing found the products contained various undeclared active ingredients, including sildenafil, tadalafil, vardenafil, sibutramine, desmethylsibutramine, phenolphthalein and/or fluoxetine. Many of these are active pharmaceutical ingredients for use in FDA-approved prescription drugs, which are restricted to use under the supervision of a licensed health care professional. Twenty-eight of these products have been voluntarily recalled during FY 2021.

FDA Warns Five Companies Illegally Selling Dietary Supplements Claiming to Treat Infertility

On May 26, 2021, FDA and the Federal Trade Commission (FTC) jointly issued warning letters to five companies for illegally selling dietary supplements that claim to cure, treat, mitigate, or prevent infertility and other reproductive health disorders in violation of the Federal Food, Drug, and Cosmetic Act (FD&C Act). These companies were selling and marketing their products

with unproven claims online and through their social media accounts. See <https://www.fda.gov/news-events/press-announcements/fda-ftc-warn-five-companies-illegally-selling-dietary-supplements-claiming-treat-infertility>.

FDA Online Opioid Summit

On September 9, 2021, FDA virtually hosted its third summit to continue to enhance collaboration to maximize the scope of our efforts to address the illegal availability of opioids online. The focus of the summit was enhancing collaboration with internet stakeholders, government entities, academia, and other important partners. Discussions at the summit highlighted successes since previous summits and discussed new ways to continue to combat the online component of the opioid crisis.

Enforcement Actions

The FDA Office of Criminal Investigation's Cybercrime Investigations Unit (CcIU) continues to target darknet marketplaces and vendors that manufacture and sell counterfeit opioids, by identifying those responsible, arresting perpetrators, and seizing manufacturing equipment, counterfeit drugs, and assets. Thus far, CcIU's Operation CyberPharma has led to the arrest of 46 darknet vendors and aided in the takedown of a major darknet marketplace as well as the seizure of drug counterfeiting tools, counterfeit drugs, and over \$6.9 million in virtual currencies and other assets. CcIU agents also monitor the surface web to identify sellers of counterfeit FDA-regulated products. Cybercrime agents can swiftly make test purchases from online merchants selling consumer goods suspected to be counterfeit or substandard. In response to the COVID-19 pandemic, CcIU agents have participated in Operation Quack Hack, an FDA-wide initiative targeting counterfeit or substandard COVID-19 related products. Since its inception in March 2020, this operation has resulted in the removal of approximately 2,100 fraudulent or unproven products by domain name registrars and marketplaces. Cybercrime agents have used this operation in support of a number of COVID-related criminal cases, including the identification of counterfeit masks and the closure of a website claiming to sell the Moderna COVID-19 vaccine.

Pilot Process to Reduce the Availability of Opioids Online Launched

In June 2020, FDA and the National Telecommunications and Information Administration (NTIA) partnered to announce the launch of a 120-day pilot to help reduce the availability of unapproved opioids illegally offered for sale online. Under the pilot, the FDA notified participating internet registries – Registry Services (formerly Neustar), Verisign, and Public Interest Registry – when the agency sent a warning letter to a website operator and the website operator did not respond adequately within the required timeframe. The internet registries reviewed the FDA's notifications and assessed whether to take further voluntary action, including possible domain name suspensions or blocks. As a result of the pilot, nearly 30 websites illegally offering opioids for sale became inaccessible to the public.⁴

⁴ FDA In Brief: FDA Continues Efforts to Curb Illegal Availability of Unapproved Opioids Online, February 1, 2021 available at: <https://www.fda.gov/news-events/fda-brief/fda-brief-fda-continues-efforts-curb-illegal->

Consumer Education

The FDA/Center for Drug Evaluation and Research's ongoing [*BeSafeRx: Know Your Online Pharmacy*](#) campaign raises awareness about the dangers of buying prescription medicine from illegally-operating online pharmacies. This campaign helps consumers understand the risks, identify the signs of an unsafe online pharmacy, and identify the signs of a safe online pharmacy.

During FY 2021, the BeSafeRx campaign received 2,039,602 airings/placements, yielding an estimated 294.74 million impressions across TV, radio and waiting rooms. This includes the BeSafeRx TV public service announcements (PSAs) which aired 21,471 times on 194 television stations and 10 television networks across the country, yielding approximately 113.27 million impressions.

The BeSafeRx radio PSAs aired 53,229 times on 940 radio stations (unique stations including Nielsen, non-Nielsen, and Total Traffic & Weather Network affiliates), 13 networks (including TTWN) and 1 program, yielding approximately 167 million impressions.

The BeSafeRx video PSAs also aired 1,964,902 times in the waiting rooms of physician offices and hospitals across the country, yielding 14.47 million impressions.

Outreach to Health Care Providers

FDA provides various online courses to inform healthcare professionals and provide them continuing education opportunities. One of these courses, *Tainted Products Marketed as Dietary Supplements*, is available for access through the FDA website. The course focuses on the prevalence of adulterated and misbranded products masquerading as dietary supplements sold in convenience stores, retail establishments, and online. These products continue to be the source of adverse event reports submitted to the agency. The webinar outlines how healthcare professionals can help protect consumers and patients from these products, how adverse events can be reported to FDA, and what measures FDA is taking to protect consumers and patients.

Using Advanced Technology to Identify Suspect Products: CDx (handheld Counterfeit Detection devices)

FDA scientists developed a handheld Counterfeit Detection (CDx) device intended to be used to rapidly screen suspect products and packaging, by visualizing differences between suspect and authentic products and providing preliminary findings in the field. The current CDx technology is used at the U.S. International Mail Facilities (IMFs) to screen incoming packages to assess finished dosage form pharmaceuticals that are offered for entry.

The goal is to put affordable tools for identifying counterfeit FDA-regulated products, including pharmaceuticals, in the hands of global regulatory law enforcement, and public health officials.

[availability-unapproved-opioids-online](#). Please note the pilot was directed to websites offering misbranded and/or unapproved opioids for sale to U.S. consumers and did not specifically address counterfeits.

An updated device prototype, CD5, is currently being evaluated for field-screening suspected counterfeit pharmaceuticals, and intelligent sampling of products for further examination and confirmation/analysis. Information gathered during a pilot study will be used to finalize the device production units and to refine the training program and materials to support their use.

In FY 2021, 66 examinations were conducted by import investigators using the CDx devices. The 66 products examined with the CD5 represented over 9,400 individual finished dosage form pharmaceuticals from four IMFs. 29 of the 66 different products were sent to the Forensic Chemistry Center for confirmation and/or analysis.

Scientific presence and field deployable tools for rapid field detection of illegal, unapproved, and counterfeit pharmaceuticals and tainted supplements

In October 2020, FDA, with DHS/CBP and DHS/ICE Commissioners formalized a partnership at International Mail Facilities (IMF) in a Memorandum of Understanding. This agreement increases collaboration to maximize inspection and detection capabilities in order to prevent illegal and harmful products entering the U.S. through the nation's IMFs and Ports of Entry. This partnership includes an increase in scientific resources at selected IMFs and sharing of space, technologies and information, which will facilitate mission responsibilities by improving efficiency and reducing duplication of efforts.

FDA's Office of Regulatory Affairs (ORA) identified specially trained field-based scientists using an established a set of tools to be the most scientifically reliable and efficient approach for the rapid identification of illicit FDA-regulated products (such as counterfeit drugs, including opioids, and adulterated "supplements"). ORA expanded collaborative efforts with Federal partners in the fight against illegal/unapproved drugs by establishing satellite laboratory presence at the Chicago O'Hare IMF in partnership with CBP's Laboratories and Scientific Services (LSS) and by continuing method development work on detection of pharmaceutical based agents. Additionally, in 2021 ORS and OEIO provided training and deployed a handheld Raman device, which can be used to identify illegal/unapproved drugs at ports of entry. While COVID interrupted IMF lab operations in 2020, in May 2021 FDA's Forensic Chemistry Center trained additional scientists and resumed full operations at the Chicago IMF. FDA's plans continue to move forward to have additional IMF satellite laboratories operational in FY 2022.

Collaboration with CBP at international mail facilities (IMFs)

As part of FDA's Import Operation Strategy, FDA import operations personnel work daily with U.S. Customs and Border Protection (CBP) personnel at IMFs and ports of entry. FDA regulatory investigators determine admissibility of FDA-regulated products. All parcels reviewed that contain pharmaceuticals, regardless of detention status, are documented and processed by FDA. On a daily basis, FDA generates data at seven IMFs regarding the detention of unapproved drugs, suspected counterfeit pharmaceuticals, products marketed as foods and/or dietary supplements containing undeclared active pharmaceutical ingredients, and other non-compliant FDA-regulated products. This data is routinely shared within FDA and CBP.

FDA also shares technology with CBP. For example, FDA and CBP personnel collaborate to utilize FDA's handheld CDx (discussed above) to identify counterfeit pharmaceuticals. FDA's Office of Enforcement and Import Operations in cooperation with the Office of Regulatory Science is looking at extending the CDx in conjunction with other handheld technologies to identify additional potential counterfeit pharmaceuticals and FDA-regulated products containing undeclared APIs. For example, the first training sessions for OEIO field staff and OCI on the Progeny ResQ, a handheld Raman device, were held in May 2021, with advanced training planned for FY 2022. The Progeny is also used by IMF satellite lab chemists to complement the CDx for identification of counterfeit pharmaceuticals. The Progeny can identify potentially misbranded and adulterated drug products, assist investigators/inspectors in making sampling decisions, and add a margin of safety for inspectors by permitting some identifications to be accomplished on intact containers.

International Capacity Building and Training: FDA Capacity Building and Training

Below are examples of FDA's Office of Criminal Investigations (OCI) capacity building and training activities with foreign countries.

In October 2020, OCI participated in the virtual 27th Meeting of the Heads of Medicines Agencies Working Group of Enforcement Officers (WGEO). WGEO was established in 2007 by the Heads of Medicine Agency to contribute to the protection of human and animal health welfare.

In October 2020, OCI participated in the Indo-Pacific Regional Webinar Series on Enforcement against Trade in Counterfeit Goods. The session on *Overview of Laws against IP Infringement and Challenges for Consumers and Rightsholders in the Global and Online Environment* was hosted by the Department of Justice (DOJ) and the U.S. Patent and Trademark Office (USPTO).

In November 2020, OCI participated in the Indo-Pacific Regional Webinar Series on Enforcement against Trade in Counterfeit Goods. The session on *Transnational Enforcement Operations: How Law Enforcement and Public Prosecutors Can Work with the Private Sector* was hosted by DOJ and USPTO.

In December 2020, OCI conducted a liaison and outreach meeting with representatives from the United Kingdom's National Crime Agency, Border Force, and Her Majesty's Revenue, together with CBP and Homeland Security Investigations, to discuss information sharing on U.S./U.K. criminal investigative leads involving unapproved/counterfeit COVID-19 Vaccines.

In January 2021, OCI participated, via teleconference, in a training workshop with Bayer AG on *Crime Defense Meeting* that focused on combatting transitional crime involving FDA regulated products and the associated public health risk.

In February 2021, OCI, and FDA's Europe Office met with the European Union's (EU) executive body, known as the European Commission (EC). The focus of the initial meeting was to make the EC aware of issues FDA faces regarding the EU's Falsified Medicines Directive and

the issue of non-FDA approved products being shipped to the United States from and through the EU. Further meetings and dialogue are anticipated.

In February 2021, the OCI liaison to Europol initiated meetings with the Universal Postal Union (UPU) located in Berne, Switzerland. These meetings, in conjunction with the U.S. Postal Inspection Service, have focused on steps that can be taken to enhance the effectiveness of the prohibited-items list as it relates to small mail parcels containing violative FDA regulated products being shipped to the United States.

In March 2021, OCI participated, via teleconference, in the 9th Annual Pharma Anti-Counterfeiting & Serialisation 2021 regarding counterfeit medical products in light of the COVID-19 pandemic.

In March 2021, OCI participated, via teleconference, in the Anglophone Pharmacrime Working Group with DOJ and discussed a case study on *Investigating Large Criminal Networks*. The participants analyzed investigative and prosecutive techniques from an FDA perspective.

In March 2021, OCI participated, via teleconference, in an annual workshop hosted by the Organization for Economic Co-Operation and Development's Task Force on Countering Illicit Trade. The workshop was on *Countering Illicit Trade for Strong Recovery*.

In March 2021, OCI liaison to Europol attended the virtual "kick-off" meeting for Operation Shield II. Operation Shield is funded by the EU's Intellectual Property Office (EUIPO) and coordinated by Europol. This year's operation will focus on a variety of medical products and will be led by several European countries. It is also supported by the EU's European Anti-Fraud agency (OLAF).

In May 2021, OCI participated, via teleconference, in a workshop held by the African Regional Intellectual Property Organization, on *Combating Counterfeit Food and Beverages*.

In May 2021, OCI participated, via teleconference, in a workshop hosted by DOJ for Bulgarian Customs. The participants analyzed investigative and prosecutive techniques from an FDA perspective.

In May 2021, OCI participated, via teleconference, in a workshop hosted by DOJ for the Africa Joint Pharmacrime Working Group. The participants analyzed investigative and prosecutive techniques from an FDA perspective.

In May 2021, OCI participated, via teleconference, in a workshop with the U.K.'s Medicines and Healthcare products Regulatory Agency (MHRA) and the National Food Crime Unit (NFCU) on *Basic online undercover purchases*. The training introduced MHRA and NFCU to OCI's investigative experience in handling illicit online pharmacy investigations, and incorporated threat assessments and evaluations involving emerging drug supply chain issues, public health threats, and the infrastructure that supports this type of criminal activity.

In May 2021, OCI participated, via teleconference, in a workshop hosted by USPTO on *Combating the Distribution and Sale of Counterfeit Medicines and Vaccinations* for officials from Mexico, Guatemala, Honduras, and El Salvador.

In June 2021, OCI participated, via teleconference, in a workshop hosted by USPTO on *Intellectual Property and Health* for Mexican prosecutors and law students.

In August 2021, OCI successfully completed a six-month virtual training workshop for a broad range of officials from Pakistan Customs Service (PCS). The workshop, which was co-hosted with the USPTO and the Commerce Department's Commercial Law Development Program, enhanced the capacity of PCS to help protect drug supply chain from the threat of counterfeits and identify trends and patterns of transnational criminal organizations exploiting trade routes. The program continued to build and strengthen the relationship between and among the participants, including the use of an interagency approach for addressing intellectual property rights, collaborating on enforcement issues, and protecting public health and safety.

Laboratory/Analytical Capacity Building through International Collaboration

The International Laboratory Forum on Counterfeit Medicines (ILFCM) is comprised of scientific experts from National Regulatory Control Laboratories. It began in 1999 with a bilateral arrangement between FDA and the United Kingdom's Medicines and Healthcare products Regulatory Agency (MHRA), and it developed into a partnership with global regulatory counterparts from Europe, North America, Asia, and Australia to maximize the benefits of a scientific network and exchange information on emerging issues related to counterfeit and illegal medicines. The ILFCM also focuses on issues related to falsified/substandard medicines, adulterated dietary supplements, and other important public health topics. The ILFCM is closely aligned with the Permanent Forum on International Pharmaceutical Crime (PFIPC) and provides scientific guidance and laboratory support.

The 2020 and 2021 annual PFIPC/ILFCM meetings were cancelled due to the COVID-19 global pandemic. At this time no decision has been made on the 2022 meeting.

Enforcement Activities

OCI's Cybercrime Investigation Unit (CcIU)

OCI's internet-related criminal investigations are led by its Cybercrime Investigations Unit (CcIU), which strategically targets online transnational criminal networks that threaten the public health of Americans. In FY 2021, CcIU focused resources to counter public health threats, such as the COVID-19 pandemic and the opioid crisis, through enforcement operations such as Operation Quack Hack and Operation Cyber Pharma (described above). CcIU also participates in the Permanent Forum on International Pharmaceutical Crime (PFIPC), the Public Safety Working Group of the Internet Corporation for Assigned Names and Numbers (ICANN) Governmental Advisory Committee (GAC), and several cybercrime-related international law enforcement working groups.

OCI's International Operations Program

OCI's International Operations Program (IOP) assists in detecting violative shipments of FDA-regulated products entering our domestic ports and facilities. It is led by two Senior Operations Managers and consists of 16 full-time and one part-time IOP special agents and supported by two intelligence research specialists. IOP's priorities include responding to U.S. Postal Service International Mail Facilities (IMFs), express consignment carrier facilities (including integrators such as DHL, UPS, and FedEx), air cargo facilities, and sea and land ports. IOP special agents routinely conduct joint enforcement activities, including internationally, and play a critical role as part of the FDA's support to the U.S. government-wide effort to combat cross-border crime.

IOP frequently provides training to its foreign law enforcement counterparts. In FY 2021, IOP successfully completed a six-month virtual bilateral training workshop and joint exercise for the Pakistan Customs Service, together with the Commerce Department's Commercial Law Development Program and the U.S. Patent and Trademark Office. The focus of this workshop was to help identify, interdict, and seize contraband transiting through air freight and air mail facilities in Pakistan that poses a significant health and safety risk for the public in the United States, Pakistan, and elsewhere. IOP also provides training to federal partner agencies, State and local law enforcement personnel, and regulated industry.

OCI Enforcement Actions

OCI plays a leading role in combating counterfeit pharmaceuticals and medical devices. Below are notable examples of OCI's enforcement activities. Additional FDA enforcement cases are discussed further below.

Review of Certain Imported Drugs

FDA has implemented the enforcement tool provided by section 708 of the Food and Drug Administration Safety and Innovation Act (FDASIA) to combat illegal drug importation. Section 708 amended section 801(a) of the FD&C Act to give FDA the authority to administratively destroy refused drugs that are valued at \$2500 or less. This authority was implemented nationwide in FY 2017.

In addition, in the SUPPORT Act (Substance Use-Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act), which became law on October 24, 2018, Congress granted FDA additional imports authorities to help the Agency advance efforts to stop illegal and unsafe drugs from being imported into the United States. For instance, section 3022(d) of the SUPPORT Act added section 801(u) to the FD&C Act; the provision authorizes FDA to treat certain imported articles as "drugs" for purposes of determining admissibility, including if the article is an ingredient "that presents significant public health concern" and it is, or contains, the same active pharmaceutical ingredient of an FDA approved drug. This provision enhances FDA's ability under its importation authorities in section 801 of the Act to detain, refuse and/or destroy illicit articles imported in the IMFs.

FDA developed procedures for the section 801(u) authority and began using this new authority on March 4, 2019. In FY 2020, FDA destroyed over 34,000 violative drug products that were not in compliance with U.S. requirements. More than 22,000 (65%) of those violative drug products were destroyed based on the new authority under section 801(u). In FY 2021, FDA has destroyed over 59,000 violative drug products with more than 43,000 (73.7%) utilizing this authority.

The Safeguarding Therapeutics Act

In the Safeguarding Therapeutics Act (Pub. L. 116-304), signed into law on January 5, 2021, Congress amended section 801(a) of the FD&C Act to grant FDA the authority to administratively destroy medical devices valued at \$2500 or less (or such higher amount as the Secretary of the Treasury may set by regulation) that have been refused admission into the United States. FDA is in the process of implementing this new destruction authority with development of the associated regulation.

Operation Opson

FDA continues to participate in the annual **Operation Opson**, which is a joint operation lead by Europol and INTERPOL that targets counterfeit and substandard food and beverages. **Operation Opson** began in 2010 and has grown to include over 60 participating countries.

Other FDA Enforcement Actions

In addition to the operations discussed above, FDA-led enforcement cases during FY 2021 include the following prosecutions:

Pennsylvania Man Sentenced to 70 Months' Imprisonment for Trafficking Counterfeit Drugs. Stefen Knoche of Lebanon, Pennsylvania, was sentenced to 70 months' imprisonment by U.S. District Court Judge Sylvia H. Rambo for trafficking in counterfeit drugs. Knoche was also ordered to pay \$3,648,911.18 in restitution. Knoche previously admitted that he 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 2017 and April 2018. Knoche further acknowledged that he trafficked counterfeit Viagra, Aurogra, Xanax, Levitra, Cialis, and Valium, all using counterfeit trademarks of their respective pharmaceutical companies. <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/press-releases/lebanon-county-man-sentenced-seventy-months-imprisonment-trafficking-counterfeit-drugs>

Man Sentenced for Selling Counterfeit Vapes. Christopher A. Reyes was sentenced 11 months in jail and a 12-month probationary period after pleading guilty to selling counterfeit vape pens imported from China. Reyes admitted that he allowed employees of a vaping shop to order counterfeit THC vaping products online using his banking information. In September 2019, CBP agents intercepted a shipment of 2,400 counterfeit THC vaping devices addressed to Reyes bound for his home. The vaping devices, which were sent from China and routed through DFW International Airport, bore the counterfeit trademark of a popular THC vape brand, "Cookies."

Agents estimated that at least five additional shipments of vaping products had been sent to Reyes. Reyes admitted that after receiving the packages, he sold the contents back to the vaping shop for profit.

<https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/press-releases/man-pleads-guilty-selling-counterfeit-vapes>

Alabama Couple Sentenced for Producing Fake Prescription Drugs. A Bessemer, Alabama, married couple were sentenced by U.S. District Court Judge Annemarie Axon for possessing pill presses used to make fake prescription drugs. Earnest Lee Coleman was sentenced to 78 months in prison and Tashana Sims was sentenced to 36 months' probation for their roles in the offenses. Coleman pleaded guilty to possessing punches, dies, and plates with the intent to defraud or mislead, being a felon in possession of a firearm, possessing controlled substances with the intent to distribute them, holding for sale and dispensing a counterfeit drug, and adulteration of a drug. Sims pleaded guilty to illegally possessing punches, dies, and plates. In April 2018, an international mail package from China was intercepted en route to the home of the defendants. The package contained two metal dies and a metal mold designed to be used to produce pressed pills. Authorities searched the defendants' home, finding controlled substances, multiple firearms, a pill press, and powders and dyes used to make fake drugs. In October 2019, authorities again searched the home, finding an additional pill press, punch and die, and firearms. Evidence disclosed the defendants ran a counterfeit prescription pill operation out of their home in which Coleman used acetaminophen, fentanyl, heroin, and paverine to make pills similar in appearance to legitimate pharmaceuticals with markings such as "Lortab," "Adderall," "Soma," "Xanax," "Ecstasy," "Oxycodone," and "OxyContin." <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/press-releases/bessemer-couple-sentenced-producing-fake-prescription-drugs>

Woman Sentenced for Selling Counterfeit Contact Lenses. Yonvoshkia Brown was sentenced to 36 months' probation and ordered to pay restitution in the amount of \$4,132 after pleading guilty in U.S. District Court for the Western District of Kentucky to one misdemeanor count under 21 USC §331(a) for the introduction of misbranded medical devices into interstate commerce. Brown, a sell.com member, was identified as an illicit distributor of contact lenses. Through a series of undercover online purchases, counterfeit Freshlook Colorblends (contact lenses) were obtained from Brown. The Forensic Chemistry Center determined that the counterfeits purchased from Brown – which were labeled as "sterile," and not manufactured by Novartis – were contaminated with bacteria and other living micro-organisms.

New York Man Sentenced for Trafficking of Counterfeit Tobacco Products. Jagtar Chadha was sentenced to one year in prison and three years of supervised released, as well as ordered to pay \$1.6 million in restitution and forfeit \$431,000 after pleading guilty in U.S. District Court for the Southern District of New York to Trafficking in Counterfeit Goods (18 USC § 2320. In March 2017, OCI became aware of counterfeit tobacco trafficking by a company named DC Distributors located in Hicksville and New York, New York. Local law enforcement used an informant to purchase counterfeit Logic-branded electronic-delivered tobacco from a DC Distributors warehouse. Two months later, FDA intercepted a large shipment entering the U.S., and destined for DC Distributors, of counterfeit Logic tobacco products from China. In November 2018, June 2019, and July 2019, through an informant, OCI purchased counterfeit

Logic brand electronic tobacco products, misbranded Juul products, and foreign unapproved medical products from Chadha at DC Distributors.

Florida Man Sentenced for Selling Counterfeit Drugs on the Dark Net. Benjamin Burdick was sentenced to three years in prison in the U.S. District Court for the Eastern District of Virginia for the sale of counterfeit drugs in violation of 21 USC § 331(i)(3) and § 333(b)(8), and the use of a counterfeit mark in connection with trafficked drugs in violation of 18 USC § 2320(a)(4). 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 contained alprazolam, which genuine Xanax contains, and the pills also contained substances such as flualprazolam, etizolam, adinazolam, and microcrystalline cellulose. <https://www.justice.gov/usao-edva/pr/florida-man-sentenced-selling-counterfeit-drugs-dark-net>

DEPARTMENT OF HOMELAND SECURITY

Department of Homeland Security

Department of Homeland Security Appendix for FY 2021 Annual Report

This appendix discusses the FY 2021 activities of the Department of Homeland Security (DHS). As outlined below, DHS's activities including protecting public and private acquisition supply chains from counterfeits; conducting law enforcement operations; engaging with stakeholders; educating the public; cooperating with foreign law enforcement; enhancing IP enforcement through international organizations; and providing capacity building and training to support IP enforcement in other countries.

Protecting Public and Private Acquisition Supply Chains from Counterfeits

Counterfeiting is a significant challenge that can impair supply chains for both the public and private sectors. This challenge has increased with the rise of e-commerce, as DHS explained in its January 2020 report on *Combating Trafficking in Counterfeit and Pirated Goods*.

In the context of the U.S. Government, acquiring products or services from sellers with inadequate integrity, security, resilience, and quality assurance controls create significant risks, from a national security and mission assurance perspective, as well as from an economic standpoint (due to the increased costs to American taxpayers). Counterfeiting can have significant consequences for the Department of Defense (DoD) supply chain by negatively affecting missions, the reliability of weapon systems, the safety of the warfighter, and the integrity of sensitive data and secure networks.

The goal is to reduce the risk of counterfeits entering the supply chain; quickly and collectively address those that do enter the supply chain; and strengthen remedies against those who provide counterfeit items.

DHS Training for Acquisition Professionals

Buyers in the public and private sectors need better visibility into and understanding of (1) how the products, services, and solutions they buy are developed, integrated, and deployed, and (2) the processes, procedures, and practices used to ensure the integrity, security, resilience, and quality of those products and services. This requires understanding the threat that counterfeits pose, mitigating their purchase and distribution, and identifying counterfeits and reporting them.

To address the systemic threat from counterfeits, the U.S. Immigration and Customs Enforcement-led National Intellectual Property Rights Coordination Center (IPR Center) provides educational opportunities for public and private acquisition professionals. The IPR Center has coordinated with the ICE Chief Financial Officer to provide this training to all purchase card holders across the agency. Additionally, the IPR Center has posted free training on its website that is designed to provide acquisition professionals with the knowledge and skills they need to combat the counterfeit threat. The training on *Acquisition Professional Training: Counterfeit Awareness, Mitigation, Identification, and Reporting* is at <https://www.iprcenter.gov/file-repository/acquisition-professional-training-1.pdf/view>.

China Working Group

In 2020, DHS formed a China Working Group, made up of senior representatives of all DHS Components, with the goal of developing an action plan to protect and defend the nation against threats from the government of China sponsored online activities. The Working Group is overseen by the Senior Official Performing the Duties of the Under Secretary for Policy and has compiled a preliminary round of actions. In January 2021, DHS issued a report *DHS Strategic Action Plan to Counter the Threat Posed by the People's Republic of China*, which documented the findings of the group.

The Working Group was sub-divided into five workstreams, which were operated at the staff level and managed by Component representatives. Of these, a representative from the Cybersecurity and Infrastructure Security Agency (CISA) manage the Cybersecurity and Critical Infrastructure workstream. Participation included staff from multiple CISA Divisions, U.S. Immigration and Customs Enforcement (ICE), U.S. Secret Service, Science and Technology, and Intelligence and Analysis. The Cybersecurity and Critical Infrastructure workstream was tasked with leading the development of action items in these relevant areas, including the prevention of intellectual property (IP) theft. The workstream generated actions related to increasing public and private sector engagement through awareness, training, and exercises; support for the granting of the administrative subpoena authority to CISA; facilitation of the protection of cloud service providers, which have been used as a vector for Chinese government-sponsored offensive attacks; augmenting support for the U.S. academic sector, which holds significant IP data and is therefore a key target; studying the effect of emerging technologies, including Unmanned Aerial Systems (UAS) manufactured in China, on the vulnerability of IP and developing deterrence strategies; and developing a strategy to protect and defend U.S. IP from Chinese government-sponsored cyber espionage and data theft. The workstream also developed milestones for each of these areas.

Law Enforcement Efforts to Secure the USG Supply Chain (Operation Chain Reaction)

In addition to the steps taken to secure the front end of the U.S. Government's supply chain (through Federal procurement regulations, supplier requirements, and acquisition training), the U.S. Government is also committed to protecting its vital interests by taking robust enforcement measures against those who sell counterfeit goods to the U.S. Government.

Operation Chain Reaction targets counterfeit items entering the military and U.S. Government supply chains, and is an IPR Center-coordinated effort led by ICE Homeland Security Investigations (HSI) and consists of 17 Federal law enforcement agencies (including HSI, U.S. Customs and Border Protection (CBP), and DoD's criminal investigative offices). In FY 2021, under ***Operation Chain Reaction***, HSI initiated 31 criminal investigations, conducted 2 criminal arrests, and helped secure 1 indictment and 3 convictions, as well as 90 seizure incidents of counterfeit goods.

Other notable ***Operation Chain Reaction*** activities during FY 2021 included the following.

- On October 14, 2020, members of the IPR Center ***Operation Chain Reaction*** Task Force co-hosted the Counterfeit Microelectronics Working Group (CMWG) led by DOJ, Computer Crime and Intellectual Property Section (CCIPS). This marked the first time the meeting was conducted as a virtual meeting due to the ongoing pandemic. The meeting primarily focused on trends in counterfeit electronic parts, but also highlighted a successful prosecution of an individual for knowingly engaging in criminal behavior which potentially could have introduced counterfeit microelectronics into the United States Space Program.

Law Enforcement Operations

Protection and enforcement of IPR is a national priority, and U.S. law enforcement stands at the forefront of these efforts.

As of September 30, 2021, CBP and ICE made 27,115 IPR seizures. The total estimated manufacturer's suggested retail price (MSRP) of the seized goods, had they been genuine, was about \$3.3 billion.

In addition to ***Operation Chain Reaction*** (discussed above), the DHS law enforcement efforts during FY 2021 included the following operations:

Operation Apothecary

Operation Apothecary is the IPR Center's public health and safety initiative that addresses, analyzes, and attacks potential vulnerabilities in the entry process that might allow for the smuggling of commercial quantities of counterfeit, unapproved, and/or adulterated drugs through international mail facilities, express courier hubs, and land borders.

On June 16, 2021, IPR Center personnel presented at the Drug Enforcement Administration's Chemical Industry Conference which was attended by approximately 200 representatives from private industry. The IPR Center provided a briefing on investigative programs and priorities with a focus on protecting pharmaceutical companies' intellectual property.

During FY 2021, under ***Operation Apothecary***, HSI initiated 49 criminal investigations, 19 arrests, 25 indictments, and 21 convictions, as well as 204 seizure incidents of counterfeit items.

E-Commerce/Operation in Our Sites

The E-Commerce Program is an on-going HSI initiative targeting entities that sell counterfeit products through the internet. This program consists of the well-known operation, ***Operation in Our Sites*** (IOS), which was initiated in 2010 as a method to disrupt this activity online. The E-Commerce initiative focuses on developing long term investigations that identify targets, assets, and financial schemes used in operating infringing websites devoted to trafficking in infringing materials. It also emphasizes working in partnership with third-party entities, such as online

marketplaces, payment processors, and the express consignment industry. Additionally, the IPR Center coordinates with rightsholders, who utilize civil and administrative remedies to shutdown infringing sites.

In recognition of the wide reach of e-commerce into many of its programmatic areas, HSI promulgated a single agency strategy on February 14, 2018. The HSI E-Commerce Strategy emphasizes an agency approach that leverages collaboration between private industry and law enforcement partners in an effort to act as a force-multiplier in a cooperative enforcement approach to identify and dismantle organizations, and to prosecute persons or entities, that traffic in all manners of dangerous and illicit goods utilizing various e-commerce outlets including open-net websites, the dark web, point-to-point sales platforms, social media, and a variety of payment processors and shipping methods.

In FY 2021, in furtherance of the e-Commerce Strategy, IPR Center personnel conducted several meetings with representatives from online platforms, payment processors, and the shipping industry for the purpose of furthering dialogue about how to share information for the purpose of stopping the online sale of counterfeit goods.

On April 21, 2021, the IPR Center presented at a virtual Organization for Economic Cooperation and Development (OECD) Task Force on Countering Illicit Trade working group on the challenges of e-commerce and illicit trade. The IPR Center discussed the E-Commerce Working Group and the Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION), including successes and challenges moving forward. Participants included law enforcement representatives from the UK, and Australia, and OECD personnel.

In FY 2021, **under E-Commerce/IOS**, HSI initiated 19 criminal investigations, conducted 2 arrests, and helped secure 1 indictment and 2 convictions. These investigations are initiated and developed by HSI field offices through IPR Center leads, seizures, informants, complaints, industry leads, and/or other investigative techniques.

IOS Cyber Monday/Project Transatlantic

Under ***IOS Cyber Monday/Project Transatlantic***, the IPR Center – through HSI – partners with Europol to leverage its member countries to launch multilateral enforcement actions against targeted websites and their operators illegally selling counterfeit merchandise. The operation involves the execution of coordinated seizures of domestic and foreign-based internet domain name registrations in the United States and Europe. Through the ongoing international Operation “In Our Sites,” the IPR Center and Europol seized or shut down more than 490,475 websites illegally selling counterfeit goods and other copyright-protected material to unsuspecting consumers between November 2020 and November 2021.

Operation Engine Newity

Operation Engine Newity (OEN) is an HSI-led, IPR Center initiative that focuses on securing the supply chains of automotive and other heavy industry from counterfeit components. The proliferation of counterfeit parts - including critical components such as airbags, bearings, brake pads, accelerator arms, and windshields - has grown exponentially over the last several years and

now poses a significant health and safety threat to end users and an economic cost to businesses and consumers through lost revenue, downtime, and replacement costs.

OEN personnel work closely with automotive original equipment manufacturers (OEMs), aftermarket parts manufacturers and suppliers, and other automotive parts and equipment companies, including members of the Automotive Anti-Counterfeiting Council (A2C2) and the Automotive Aftermarket Suppliers Association (AASA) Intellectual Property Council. The companies support criminal investigations by providing case support and product authentication.

- On March 12, 2021, the IPR Center coordinated with Force Pierce HSI for ***Operation Engine Newity*** on targeting the importation and trafficking of counterfeit automotive merchandise. On May 25, 2021, HSI Fort Pierce executed a federal search warrant resulting in the seizure of approximately 17,089 items with an estimated MSRP value (if genuine) of \$3 million.
- On April 9, 2021, the IPR Center coordinated with HSI Las Vegas for ***Operation Engine Newity*** on targeting the importation and trafficking of counterfeit automotive merchandise. On June 12, 2021, HSI Las Vegas executed a Nevada state search warrant resulting in the seizure of 18,720 items with an estimated MSRP value (if genuine) of \$2.8 million.
- In November 2019, ***Operation Engine Newity*** brand partners notified HSI Phoenix regarding counterfeit SD cards with updated GPS navigation map systems. On May 19, 2021, HSI Phoenix executed a search warrant resulting in the seizure of 3,000 counterfeit items with an estimated MSRP value (if genuine) of \$1.5 million.

In FY 2021, under ***Operation Engine Newity***, HSI initiated 21 criminal investigations, conducted 6 criminal arrests, and helped secure 4 indictments and 6 convictions, as well as 55 counterfeit goods seizures incidents with an estimated MSRP value (if genuine) of approximately \$26.6 million.

Operation Surge Protector

Operation Surge Protector (OSP) was initiated by the IPR Center in December 2016 to target the sale and trafficking of counterfeit consumer electronics and technology products, such as batteries, chargers, smartphones, and charging cords. OSP combines the expertise of HSI, CBP and the Consumer Product Safety Commission (CPSC).

From August 28-September 1, 2021, representatives of OSP worked in conjunction with CBP and HSI on an enforcement operation in Anchorage, Alaska that focused on identifying counterfeit cellular phones being used in an ongoing fraud scheme.

In FY 2021, under ***Operation Surge Protector***, HSI initiated 8 criminal cases, conducted 6 arrests, and helped secure 3 indictments and 2 convictions.

Operation Body Armor

Operation Body Armor, which combines the expertise of HSI, CBP, and FDA-OCI, was initiated in January 2015 by the IPR Center in partnership with industry and other entities associated with the healthcare and beauty product community to combat the sale of counterfeit personal healthcare and beauty products.

In FY 2021, under ***Operation Body Armor***, HSI initiated 28 criminal cases, conducted 3 arrests, and seized counterfeit goods with an estimated MSRP (if genuine) of approximately \$15.95 million.

Operation Intangibles

In December 2019, the IPR Center hosted the inaugural event for ***Operation Intangibles*** at the first ever HSI digital piracy symposium. This symposium brought law enforcement and CCI experts together to address stakeholders' concerns in copyright protection and enforcement efforts. This symposium further addressed collaborative efforts in countering digital piracy to further protect a vital sector of the U.S. economy.

Through this initiative, the IPR Center collaborates with industry partners to develop effective digital piracy training for law enforcement and creates avenues of access to CCI subject matter and technical experts for investigative assistance. This initiative merges HSI's foreign and domestic investigative resources with industry partners in a global effort to counter the growth of digital piracy. Through ***Operation Intangibles***, HSI investigative and operational programs will be more effective in targeting the entire digital piracy ecosystem for disruption and dismantlement.

- On June 23, 2021, the HSI Global Trade Investigations Division, IPR Center, hosted a *Digital Piracy Virtual Training* featuring presentations from DOJ and industry partners from MPA, RIAA and BSA. The purpose of this training was to facilitate information on emerging technology, terminology, and other impact indicators specific to the industry. Attendees included investigators from HSI and FBI from field offices around the country.
- On July 8, 2021, HSI DC executed three seizure warrants for thirteen commercial website domain names offering unauthorized copyright-protected content. The enforcement action was part of a Government of Brazil-led international operation targeting digital piracy dubbed "Operation 404." This was an HSI DC led investigation with significant support from HSI Brasilia and the IPR Center; DOJ's EDVA, ICHIP and CCIPS; and Brazil entities.

Operation Team Player

Operation Team Player (OTP) targets the sale and trafficking of counterfeit sports merchandise, apparel and tickets, a multi-million-dollar criminal industry. The culmination of the sports season—playoffs and finals games—are events that stimulate the sale of counterfeit items. HSI Special Agents and CBP Officers worked with sports leagues and law enforcement agencies

throughout the nation to identify shipments of counterfeit sports merchandise being imported to the United States or being sold by vendors. In FY 2021, the IPR Center continued coordinating enforcement actions at multiple high-profile sporting events, including the National Football League (NFL) Pro Bowl and Super Bowl, Major League Baseball (MLB) World Series, National Hockey League (NHL) Winter Classic, and the National Hockey League (NHL) and National Basketball Association (NBA) All-Star games.

- On January 29, 2021, IPR Center and CBP representatives traveled to Tampa, FL to coordinate ***Operation Team Player*** enforcement operations targeting the importation and trafficking of counterfeit sports merchandise and media activities related to Super Bowl LV. As a result of these efforts, task force officers arrested 1 individual and seized approximately 15,671 items with an estimated MSRP value of \$59,496,005.
- On April 8, 2021, IPR Center representatives traveled to Tampa, FL to coordinate ***Operation Team Player*** enforcement operations targeting the importation and trafficking of counterfeit sports merchandise and media activities related to WrestleMania 37. The operations were conducted by teams comprised of HSI Tampa, HSI Dallas, IPR Center representatives, Tampa Police Department, and representatives from World Wrestling Entertainment.
- On April 23, 2021, IPR Center representatives coordinated and conducted an ***Operation Team Player*** virtual training in support of anticipated IPR enforcement operations for the 2021 NFL Draft. The training included presentations from the IPR Center and the National Football League. The training was attended by 36 representatives from HSI Cleveland and the Cleveland Police Department.
- On April 27, 2021, IPR Center representatives traveled to Cleveland, OH to coordinate ***Operation Team Player*** enforcement operations targeting the importation and trafficking of counterfeit sports merchandise and media activities related to the 2021 NFL Draft.
- On June 16, 2021, the IPR Center presented at a virtual INTERPOL seminar on *Sport and Intellectual Property*. IPR Center provided an overview of ***Operation Team Player*** including operational and investigative planning consideration for law enforcement. The seminar included presentations from law enforcement and rightsholders. Participants included law enforcement representatives from more than 70 countries.

Operation Pangea

Operation Pangea is a coordinated global effort led by INTERPOL as a means of further reducing the advertisement, sale, and supply of counterfeit, unapproved, and substandard medicines and medical devices. Websites providing counterfeit pharmaceuticals are a significant and growing global problem both from a public health and safety standpoint, as well as from an intellectual property protection standpoint. INTERPOL conducted Pangea enforcement operations from May 17-21, 2021. During FY 2021 ***Operation Pangea*** enforcement efforts, over 90 INTERPOL member countries inspected over 326,000 packages. The inspections

resulted in the seizure of over 48,000 packages, which included potentially dangerous pharmaceuticals worth over \$14 million. The operation also resulted in 121 arrests worldwide.

Operation Stolen Promise

Operation Stolen Promise was launched by HSI in April 2020 to protect the Homeland from the increasing and evolving threat posed by COVID-19-related fraud and criminal activity.

Operation Stolen Promise combines HSI's expertise in global trade, financial fraud, international operations, cyber-crime, and criminal analysis to investigate financial fraud schemes, the importation of prohibited pharmaceuticals and medical supplies, websites defrauding consumers, and any other illicit criminal activities associated with the virus that compromise legitimate trade or financial systems or endanger the public.

Operation Stolen Promise is based on the following pillars:

- *Develop Actionable Investigative and Intelligence Leads*
- *Disrupt and Dismantle Fraud Schemes, Take Down Illicit Websites and other Online Marketplaces, and Seize Counterfeit or Illicit Pharmaceuticals and Medical Devices*
- *Launch a Robust Public Awareness Campaign*

3M Investigations - Under the umbrella of ***Operation Stolen Promise*** several HSI offices are investigating individuals and organizations that are involved in the sale of counterfeit 3M N95 masks to Federal, state, and local government entities as well as hospitals and health centers. Through September 30, 2021, HSI had initiated over 134 investigative cases and seized over 28 million counterfeit masks

Under ***Operation Stolen Promise*** (as of September 30, 2021), HSI has made 3,250 COVID-19 related seizures, initiated 1,288 criminal investigations, conducted 381 search warrants, arrested 371 perpetrators, and seized over \$55M in illicit proceeds. As efforts to combat COVID-19 progress, HSI initiated Operation Stolen Promise 2.0 in November 2020 to focus on counterfeit vaccines, while continuing to investigate the trafficking of counterfeit personal protective equipment. This effort will coincide with INTERPOL's ***Operation Vigilant Interdiction***, which will also primarily focus on combatting counterfeit COVID-19 vaccines.

* * *

DHS's law enforcement activities during FY 2021 also included the following activities:

- In FY 2021, the IPR Center supported an INTERPOL webinar focusing on *Protecting Intellectual Property in the time of COVID-19* held for INTERPOL member countries. IPR Center/HSI agents discussed general IP protection and trends and lessons learned during HSI's COVID-19 response. Industry brand protection representatives from the Pharmaceutical Security Institute, Ely Lilly and Pfizer also conducted presentations.

- On July 1, 2021, the IPR Center presented at a virtual seminar on Operation Stolen Promise with HSI Beijing, the U.S. Embassy Ulaanbaatar, and Mongolian Customs, law enforcement, and prosecutors. The IPR Center provided an overview of Operation Stolen Promise including operational successes and investigative planning consideration for law enforcement. The seminar included presentations from Pfizer related to vaccines and supply chain security.
- On September 27, 2021, the IPR Center presented at a virtual seminar on Operation Stolen Promise with HSI Vietnam, the U.S. Embassy Consulate General Ho Chi Minh City, and Vietnamese Customs, law enforcement, and prosecutors. The IPR Center provided an overview of Operation Stolen Promise including operational successes and investigative planning consideration for law enforcement. The seminar included presentations from Pfizer related to vaccines and supply chain security.
- In FY 2021, HSI initiated 715 intellectual property investigations and was involved in 206 arrests, 101 indictments, and 77 convictions.
- In FY 2021, the IPR Center vetted 13,331 investigative leads; of these, 11,633 were referred to law enforcement partners. Finally, the IPR Center de-conflicted 1,698 investigative targets for partner agencies and industry.
- In FY 2021, due to the COVID-19 pandemic, the IPR Center adapted the Intellectual Property and Trade Enforcement Investigations (IPTEI) training course to the online environment, modifying the curriculum to offer an introductory version suitable for web-based learning. Four online sessions (20 training hours each) were held in FY 2021, with a total of 630 participants. (Previously, in-person courses were held at the IPR Center in Arlington, VA, between August 2016 until August 2019 with 30 attendees at each session, comprised of CBP and HSI personnel.) The IPTEI course offers advanced training with a specific focus on commercial fraud and IP theft. Presenters are CBP and HSI subject matter experts in selected topics and programs. The course is evaluated through anonymous online surveys which are used to review and enhance the training curriculum. HSI and CBP field personnel are the target audience for this training (previously managed and held by the Federal Law Enforcement Training Centers), which also supports the educational requirement of the Trade Facilitation and Trade Enforcement Act of 2015. Additional attendees may include representatives from the IPR Center partner agencies, DHS, and DOJ, as well as Task Force Officers placed within HSI field offices representing local and federal law enforcement.
- In FY 2021, the CBP Office of Trade adapted the Instructor Led Training (ILT) course material to the virtual environment. The ILT training is an introductory course for CBP officers detailing CBP's regulatory authorities and the IPR seizure process. Previously, ILT courses were hosted in-person at individual ports. However, in FY 2021, the Office of Trade IPR Division hosted six virtual ILT sessions, which were attended by approximately 170 participants. In addition, the webinar recordings have been made available online to all CBP personnel and have generated over 430 views.

- The IPR Center continues to provide overview and case studies on investigations worked with CBP at a three-day CBP trade enforcement advanced training event. Due to COVID cancellations in FY 2020, the IPR Center conducted two events with a total of 71 CBP and ICE personnel attending. In FY 2021, the IPR Center participated in four events with 224 CBP and ICE attendees. The training focuses on fines, penalties, and forfeitures, and is designed for trade enforcement coordinators and import specialists; also attending are CBP officers, paralegals, assistant port directors for trade, and entry specialists. The training course provides participants with the background necessary to evaluate and prioritize prospective trade violations (including AD/CVD), determine resource allocation and the appropriate enforcement response (including penalties and liquidated damages), and track and monitor results of enforcement actions. During each class, ICE provides an overview of the IPR Center and HSI's IPR and trade enforcement efforts.

Engaging with Stakeholders

The IPR Center forms the communications hub around which much of the interaction between private sector stakeholders and the law enforcement and regulatory communities takes place.

The January 2020 DHS report on *Combating Trafficking in Counterfeit and Pirated Goods* recommended numerous "Immediate Actions by DHS and Recommendations for the U.S. Government." Recommendation six acknowledged the work of the IPR Center E-Commerce Working Group (ECWG) and recommended the formation of the Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION). In furtherance of this objective, the IPR Center hosted three meetings in FY 2021 with 14 industry members of the ACTION group and our federal partner agencies at the IPR Center.

On October 7, 2020, the IPR Center hosted the second quarterly ACTION meeting. During this meeting, 14 ACTION members engaged in discussions concerning the Private Sector Best Practices that were outlined in the January 2020 DHS report. ACTION members provided the IPR Center with data concerning how their existing best practices aligned with any or all best practices outlined in the DHS Report.

On January 27, 2021, the IPR Center hosted the third quarterly ACTION meeting. During the meeting 14 ACTION members discussed the private sector responses received by the IPR Center with regards to existing best practices. ACTION members also discussed the definition of "high-risk" merchandise, and determined that designating a standard definition of high risk merchandise would allow ACTION members to work together more efficiently at targeting these items. As a result, the group agreed to form a High-Risk Working Group (HRWG) to further discuss this issue and develop a standard definition that the ACTION group could use moving forward.

On February 26, 2021, the HRWG held its initial meeting with seven ACTION members. The HRWG agreed that having a standard definition for high risk would be beneficial to support future investigative/operational issues they participate in. The group also discussed the importance of two-way sharing of intelligence, especially related to new trends identified by either private sector or government entities. A recommendation was made for the IPR Center to

develop a series of awareness bulletins which would share data with the private sector in three areas: High Risk, High Volume, and Trending.

U.S. Customs and Border Protection and the U.S. Chamber of Commerce Memorandum of Understanding

In May 2021, the U.S. Customs and Border Protection signed a Memorandum of Understanding (MOU) with the U.S. Chamber of Commerce (CoC), the first of its kind. This MOU underscores the importance of IPR and outlines general terms on connecting resources and sharing information between the two organizations to stop the flow of trade in counterfeit goods. This includes the exchange of information concerning known or suspected intellectual property rights violations, the intention to conduct joint training and outreach events, and joint public awareness of efforts to disrupt the trade in counterfeit and pirated goods.

CBP Product ID Guide Webinars

In FY 2021, the CBP Office of Trade hosted nineteen Product ID Guide webinars, reaching approximately 2,200 CBP and HSI personnel. These webinars are an opportunity for rightsholders to engage directly with CBP Officers to introduce their products, present key identifying marks for genuine goods, and highlight counterfeiting trends and areas of risk specific to their products. The webinar recordings and corresponding Product ID Guides are also made available online to all CBP and HSI personnel.

Operation Joint Venture and Project Trade Watch

Through the IPR Center's Outreach and Training Section, HSI engages in partnerships with the public and private sectors to combat IP infringement through its **Operation Joint Venture** (OJV) initiative. This IPR Center-led outreach initiative is designed to increase information sharing with public and private sectors to combat the illegal importation and distribution of counterfeit, substandard and tainted goods, as well as the evasion of duties. The initiative is aimed at fostering investigations into commercial fraud, including activities that threaten public health and safety and violate IP rights. Through OJV, the IPR Center engages with rightsholders, manufacturers, importers, customs brokers, freight forwarders, bonded facilities, carriers, and others to discuss the IPR Center's priorities of protecting public health and safety, the economy, and the U.S. Government's supply chain. Through outreach and public engagement, the IPR Center raises the public's awareness of the dangers of commercial fraud violations (such as those involving IP) and serves as a public point of contact for investigative leads. The IPR Center's audience includes a broad spectrum of industries and government agencies, including but not limited to the pharmaceutical, entertainment, wearing apparel, sports, electronic, and automobile industries, as well as customs bonded entities, importers, and law enforcement officials.

Project Trade Watch is HSI and CBP's outreach campaign to the importing community to facilitate informed compliance by private industry and to enhance public awareness of law enforcement efforts within the trade community. This campaign exists under the IPR Center's broader OJV initiative. Through **Project Trade Watch**, HSI and CBP field personnel provide information and red-flag indicators of potential import fraud and importer identity theft.

Other Engagements

DHS law enforcement agencies which support IP enforcement had numerous other engagements with stakeholders during FY 2021. Some of these public education and outreach efforts are described below.

The IPR Center has a unique role within HSI by serving as a one-stop shop for IP enforcement efforts. In this role, the IPR Center has regular contact with the international community, the media, Members of Congress, trade organizations, industry leaders, and the general public. In FY 2021, the IPR Center conducted 71 outreach and training events with 5,514 attendees.

In FY 2021, the IPR Center continued the monthly publication of the *IPRC Connections* newsletter to keep stakeholders up to date on the most significant IPR Center enforcement efforts and outreach activities. Additionally, the IPR Center collects, tabulates, and catalogs victim impact accounts of brand holders and consumers with the aim to show more clearly the full effect of IP infringement and trade fraud on the U.S. and global economies, public health and safety, and any related threat to government supply chains.

Throughout FY 2021, HSI – through its leadership at the IPR Center – collaborated with industry and other government agencies to present training and foster communication. Examples of this include:

- Cooperated with Underwriters Laboratories (UL, LLC) to deliver virtual training to HSI and CBP personnel, including topics such as the new UL label requirements and combating counterfeit battery products.
- Partnered with Philip Morris International (PMI) to offer virtual training in combating illicit trade in tobacco products, trafficking, finance and other criminal-related activity. Audiences included HSI special agents, analysts, task force officers, and members of the Transnational Criminal Investigative Units (TCIUs), as well as HSI overseas offices, with sessions dedicated to specific geographical regions.
- Engaged the Automotive Anti-Counterfeiting Council (A2C2) to provide case-study training addressing counterfeit automobile parts.
- Collaborated with DOJ Computer Crime and Intellectual Property Section (CCIPS) and USPTO to provide virtual training on various IP Enforcement topics and COVID-19-related fraud.
- Liaised with CBP Office of Trade in numerous virtual training opportunities in combating commercial fraud and intellectual property rights enforcement.
- During FY 2021, the IPR Center's Outreach and Training Section assisted with the coordination of approximately 7 meetings with industries and coalitions including JUUL, National Crime Prevention Council (NCPC), Philip Morris International (PMI), Practising Lawyers Institute (PLI), International Association of Chiefs of Police

(IACP), International Trademark Association (INTA), International Consumer Product Health and Safety Organization, and International Anti-Counterfeiting Coalition (IACC).

- IPR Center HSI personnel assigned to the National Cyber-Forensics and Training Alliance (NCFTA) leverage the resources and analytical tools of the NCFTA to identify domain names and networks affiliated with infringing activity in support of criminal investigations or potential civil enforcement action. (The NCFTA is a non-profit corporation that conducts real-time information sharing and analysis with subject matter experts in the public and private sectors and academia.)
- CBP's multi-faceted communication with IP stakeholders includes daily interaction with industry regarding enforcement activities, formal meetings involving both trade facilitation and enforcement efforts, and participation in numerous national trade events. CBP's stakeholder engagement includes:
 - Regular conference calls with the IPR working group of the Commercial Customs Operations Advisory Committee (COAC) and quarterly public meetings with COAC members;
 - Daily interaction with stakeholders affected by CBP's IP enforcement efforts at the ports of entry, and nationally through CBP's ten industry-aligned Centers of Excellence and Expertise (Centers), the IP-focused staff at headquarters, and the IPR Center in the Washington, DC metro area;
 - Participation in national and local trade events, industry meetings, speaking engagements, and industry-specific rightsholder roundtables.

Throughout FY 2021, CBP collaborated with industry in the form of an e-commerce task force to identify and address the complexities and challenges associated with the increases in small packages due to the worldwide proliferation of online and mobile technologies.

The DHS Private Sector Office (PSO) continues to coordinate U.S. Government-wide efforts to catalyze and support private sector and non-governmental-based counter-illicit trade activities. On the international stage, PSO seeks to coordinate conferences and workshops in key global locations (e.g., Asia, Eastern Europe, and Western Hemisphere) to collaborate on U.S. and international government efforts to bolster enforcement through the sharing of best practices and approaches for detecting and disrupting illicit trade activities. The U.S. Department of State is key to this effort as their respective Missions work with host governments to strengthen their enforcement regimes.

Educating the Public

Changing public attitudes toward infringing activities remains essential to an effective intellectual property enforcement strategy. DHS activities during FY 2021 included:

- CBP's Centers of Excellence and Expertise have been heavily involved in the development and implementation of the trade intelligence concept, a CBP effort to

establish formal linkages with the private sector to develop actionable intelligence. As part of these efforts, the Centers engage in continual dialogue, information sharing, and trend analysis (e.g., with the pharmaceutical industry) in order to safeguard the American public from substandard, counterfeit, or otherwise illegal products. CBP proactively and frequently issues national and local press releases, and social media notifications to educate the public on counterfeiting.

- In FY 2021, the IPR Center – in partnership with Michigan State University’s Center for Anti-Counterfeiting and Product Protection (A-CAPP), the U.S. Chamber of Commerce, and the Better Business Bureau, and with the assistance of the USPTO – launched *IP Protect*. The joint initiative provides resources – free of charge – to aid small to medium-sized enterprises (SMEs) in protecting themselves against IP theft, fraud, and cyber intrusion. One of the primary goals of *IP Protect* is to have special agents meet with local government and community organizations to facilitate connections with the companies that can benefit most from the initiative. Once these connections are made, special agents can communicate directly with local SMEs to raise awareness about exposures that can leave them at risk to IP loss and fraud and provide a local point of contact for reporting fraud and suspicious activity.
- In FY 2021, CBP continued the *Truth Behind Counterfeits* IPR Public Awareness Campaign to educate the public of the many harms associated with the purchase of counterfeit goods. The goal of the campaign is to make people aware that buying counterfeits is not a victimless crime and to encourage them to shop from reputable sources. Due to COVID-19, CBP pivoted its consumer education campaign to leverage existing digital platforms and utilize its relationships with trade associations and partner government agencies (PGAs) to bring awareness about the danger of counterfeit goods. This included a three-pronged approach, using traditional media avenues as well as CBP’s social media presence (e.g., Twitter, Facebook, Instagram, etc.); CBP’s IPR Website presence (including the *Fake Goods Real Dangers* campaign webpage); and CBP’s partnerships with government agencies and trade associations with a nexus to stopping trade in illegitimate goods that violate IPR of American businesses.
- To supplement the IPR Public Awareness Campaign, CBP organized and facilitated three publicly available webinars. These events took place throughout FY 2021 and emphasized the role CBP plays in stopping counterfeits from entering the United States.

Cooperating with Foreign Law Enforcement

As discussed above, DHS law enforcement agencies regularly cooperate with other Federal law enforcement agencies and with law enforcement offices in other countries. Below are especially notable examples of DHS cooperation with foreign law enforcement.

In FY 2021, as discussed above, U.S. law enforcement and Federal agencies – including the IPR Center through HSI, CBP, and FDA – participated in *Operation Pangea*, a global enforcement effort led by INTERPOL that is aimed at disrupting organized crime networks behind the illicit

online sale of fake drugs. The majority of Pangea participant countries conducted a week of coordinated enforcement efforts from May 17-21, 2021.

Through the U.S.-China IP Criminal Enforcement Working Group, DOJ and U.S. law enforcement (including HSI and FBI) maintain a steady exchange of information and case leads with Chinese law enforcement, resulting in successful operations to disrupt the manufacture of counterfeit items, such as airbags, pharmaceuticals, batteries, electronic components, and luxury items.

During FY 2021, the IPR Center was unable to physically host foreign government officials with an interest in IP enforcement at the IPR Center due to the ongoing COVID-19 pandemic. However, the IPR Center continued to engage foreign counterparts virtually in meetings and various outreach and training efforts. Among these were representatives from Australia, Canada, the Dominican Republic, Indonesia, Moldova, Mongolia, Norway, Panama, the Philippines, Thailand, and the UK.

Capacity Building and Training

DHS engages in training and capacity building programs to strengthen intellectual property awareness and enforcement internationally.

CBP provided trainers for Department of Justice and HSI-led regional international forums on IP enforcement for foreign governments. In FY 2021, this included HSI-led training in the Dominican Republic.

The IPR Center works closely with partner USG agencies, overseas attachés, and U.S. embassies to deliver training and support capacity building efforts across the globe. These efforts are conducted through multiple channels, including the interagency International Law Enforcement Academy (ILEA) program, INTERPOL programs, and the *Global Intellectual Property Rights Foreign Law Enforcement Training and Technical Assistance Initiative* that is funded through the Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL). This initiative – administered cooperatively by the IPR Center, DOJ CCIPS, DOJ OPDAT, and USPTO – is designed to complement the U.S. Transnational and High Tech Crime Global Law Enforcement Network (GLEN) in developing and delivering training and technical assistance on IPR and computer crimes to foreign partners in the investigative, prosecutorial, judicial, and customs and border enforcement areas. The initiative is designed to strengthen the enforcement capacity of these foreign partners for IPR matters involving transnational organized crime.

Through this initiative, the IPR Center, in conjunction with HSI Attaché offices, directs, organizes, and delivers regional IPR training in the form of lectures and presentations to foreign customs, police, prosecutors, and magistrates. The IPR Center training programs are typically held in person for 3-5 days and focus on the investigation and prosecution of IPR violations and associated crimes like smuggling and money laundering. (The COVID-19 pandemic had a significant impact on the IPR Center's ability to deliver these programs in the field, and many were condensed and moved to virtual platforms in FY 2021.) The training programs are interactive workshops led by subject matter experts and focus particular on health and safety counterfeited items such as pharmaceuticals, electronics, automotive parts, and health and beauty products. With the growing number of e-commerce marketplaces, the training programs also

focus on internet investigations. Private sector representatives or associations are invited to participate in many of the training programs to highlight the challenges their industry sector may face in a particular region and to highlight the necessity of government and industry cooperation.

In FY 2021, the IPR Center participated in 37 international training and outreaches in support of these programs. HSI continues to work closely with its law enforcement counterparts, particularly those who received training in IP enforcement. The following are examples of events that HSI either organized or supported via this program.

- **U.S. Embassy Riyadh Community Liaison Office – the monthly *Riyadh Rambler* – Outreach Activity**
In October 2020, HSI Attaché Riyadh coordinated with Mission Saudi Arabia's Community Liaison Office (CLO) for the inclusion of the *HSI S.T.O.P. COVID-19 Fraud* one-pager in the monthly November *Riyadh Rambler* for Mission Saudi Arabia. It was published on October 30, 2020, reaching more than 670 government and public officials in Saudi Arabia.
- **Saudi Arabia Presidency State Security Meeting – HSI Attaché Riyadh**
On October 20, 2020, HSI conducted an outreach meeting with the Saudi Arabian Presidency State Security to discuss HSI's *Operation Stolen Promise* efforts. The Presidency State Security is HSI Attaché Riyadh's counterpart with the Host Government and primary POC for information dissemination.
- **IACC Regional Dialogue Series for Sub-Saharan Africa – Virtual Webinar**
On October 28, 2020, the International Anti-Counterfeiting Coalition (IACC) hosted a webinar for rightsholders with operations in sub-Saharan Africa. An HSI Pretoria Special Agent provided an overview of HSI, the IPR Center, and HSI Pretoria capabilities.
- **DOJ ICHIP/USPTO-sponsored Indo-Pacific Regional Webinar Series on *Organized Crime, IP Theft, and Financial Crime: Prosecuting, Use of Forensics, Experts and Expert Testimony, and Sentencing* – Virtual Webinar**
On October 28, 2020, the U.S. Department of Justice's Office of Overseas Prosecutorial Development, Assistance and Training (DOJ/OPDAT) and the U.S. Patent and Trademark Office (USPTO) sponsored the fourth webinar in their Indo-Pacific Regional Webinar Series. The webinar featured a panel discussion on *Organized Crime, IP Theft, and Financial Crime: Prosecuting, Use of Forensics, Experts and Expert Testimony, and Sentencing*. An HSI Special Agent discussed investigations of organized crime as well as the importance of collaboration between investigators and prosecutors to effectively enforce IP crime. Participants included prosecutors, investigators, IPO officials, customs officers, and brand representatives from Brunei, Cambodia, Cook Islands, Fiji, Hong Kong, Indonesia, Malaysia, Micronesia, Myanmar, Northern Mariana Islands, Philippines, Singapore, Solomon Islands, Vanuatu, and Vietnam.

- **DOJ ICHIP/USPTO-sponsored Indo-Pacific Regional Webinar Series on *Transnational Enforcement Operations: How Law Enforcement and Public Prosecutors Can Work with the Private Sector* – Virtual Webinar**

On November 4, 2020, DOJ/OPDAT and USPTO sponsored the fifth webinar in their Indo-Pacific Regional Webinar Series. The webinar featured a panel discussion on *Transnational Enforcement Operations: How Law Enforcement and Public Prosecutors Can Work with the Private Sector*. An HSI Special Agent participated on the panel on behalf of HSI/IPR Center. Participants included 60 prosecutors, investigators, IPO officials, customs officers, and brand representatives from approximately 17 countries in the Indo-Pacific region.
- **ICHIP Webinar Series: Anglophone Pharmacrine Working Group in Africa – Virtual Webinar**

On November 10, 2020, U.S. Department of Justice ICHIPs hosted a pharmacrine working group webinar for prosecutors, investigators, customs, and regulators from Anglophone countries in Africa. An HSI Special Agent presented an HSI SAC Denver Counterfeit Pharmaceutical case. The program reached 26 participants from Botswana, The Gambia, Ghana, Kenya, Liberia, Malawi, Namibia, Nigeria, Rwanda, Sierra Leone, South Africa, Tanzania, Uganda, and Zambia.
- **DOJ ICHIP/USPTO-sponsored Indo-Pacific Regional Webinar Series on *Changing Attitudes & Behavior: Law Enforcement Priorities and Public Awareness Activities* – Virtual Webinar**

On November 11, 2020, DOJ/OPDAT and USPTO sponsored the sixth webinar in their Indo-Pacific Regional Webinar Series. The webinar featured a panel discussion on *Changing Attitudes & Behavior: Law Enforcement Priorities and Public Awareness Activities*. An HSI Special Agent participated on the panel on behalf of HSI/IPR Center. Participants included 47 prosecutors, investigators, IPO officials, customs officers, and brand representatives from approximately 17 countries in the Indo-Pacific region.
- **IPR Pharma Training on *Adapting Intellectual Property to Promote Innovation and Creativity in New Technologies* – Virtual Webinar**

On January 7, 2021, HSI Singapore participated in a Pfizer-led training to multiple Government of Singapore agencies. HSI provided a briefing on *Operation Stolen Promise*, discussed the public-private partnerships needed to successfully investigate IP crime and highlighted the capabilities of the IPR Center, and of HSI's Computer Crime Center (C3) and Illicit Finance and Proceeds of Crime Unit (IFPCU).
- **USPTO Webinar Series on *Adapting Intellectual Property to Promote Innovation and Creativity in New Technologies* – Virtual Webinar**

On January 14, 2021, HSI Singapore supported a USPTO-sponsored webinar series on *Adapting Intellectual Property to Promote Innovation and Creativity in New Technologies*. HSI participated in a panel discussion on challenges and strategies for IP enforcement in an online and transnational environment. This program was attended by officials from various countries in Southeast Asia (including Thailand, Myanmar,

Indonesia, Laos, Malaysia, Philippines, Timor-Leste, Vietnam, and Singapore) and the ASEAN Secretariat.

- **ICHIP/USPTO/IPR Center-sponsored meeting with the Dominican Republic, Office of the Attorney General on *Coordinating a Federal Response to IP Enforcement* – Virtual Webinar**

On March 19, 2021, the IPR Center and the U.S. Department of Justice ICHIP Panama hosted representatives from the Dominican Republic national government – including the Procuraduría General de la República Dominicana, Oficina Nacional de la Propiedad Industrial (ONAPI), Oficina Nacional de Derecho de Autor (ONDA), Dirección General de Aduana (DGA), Ministerio de Industria, Comercio y Mipymes (MICM), and the Instituto Nacional de las Telecomunicaciones (INDOTEL) – to discuss the investigative and prosecutorial framework of the Dominican Republic and ways to leverage best practices of partnering nations in strengthening IP enforcement capacity in the Dominican Republic. The IPR Center provided a presentation on the U.S. Government’s IP enforcement framework, including the IPR Center’s IP and Commercial Fraud programs (*Operation Stolen Promise*, *Operation Apothecary*, Tobacco Smuggling, Environmental Crimes, Import Safety, and others). The discussions also covered the structure of the IPR Center, Trade Enforcement Coordination Centers (TECCs), and the National Targeting Center-Investigations (NTC-I); a review of U.S. legal statutes (trade, IP, financial crimes, etc.); the ways in which U.S. law enforcement and prosecutors leverage these statutes; the IPR Center’s case initiation and lead development process; and prosecutorial considerations.

- **Department of State/USPTO-sponsored IP Enforcement Coordination Program – SE Asia – Virtual Webinar**

On March 21, 2021, the IPR Center supported webinar training hosted by the U.S. Embassy Jakarta, Department of State, and U.S. Patent and Trademark Office (USPTO). A representative from the IPR Center provided an IPR 101 and discussion of law-enforcement coordination in IP cases. The webinar was attended by more than 120 law enforcement officers from Indonesia, Thailand, and the Philippines.

- **American Chamber of Commerce and U.S. Embassy Moldova World IP Day Program – Virtual Webinar**

On April 26, 2021, the IPR Center supported a World IP Day Program hosted by the American Chamber of Commerce and the U.S. Embassy Moldova. Representatives from the IPR Center’s Intellectual Property Unit (IPU) and Outreach and Training Unit (OTU) provided presentations on intellectual property and related international trade violations in the United States that affect public health and safety, military readiness, and the integrity of the U.S. economy. The presentations focused on the strategies used by the United States to combat this threat to national security, including the necessity of leveraging both public and private partnerships in an increasingly digital and global society, and discussed best practice for combatting IP threats as they relate to e-commerce. These representatives also participated in panel discussions focused on strategies for combating online piracy and identifying counterfeit goods.

- Intellectual Property Investigations Training: Canada – Virtual Program**
 From July 13-14, 2021, the IPR Center and HSI Canada hosted a two-day, on-line training workshop focusing on the investigation and prosecution of counterfeit automotive parts, pharmaceuticals, and related topics for Canadian law enforcement and prosecutors. The first day focused on counterfeit automotive parts, the National Targeting Center – Investigations (NTC-I), and trade-based money laundering (TBML). The second day focused on counterfeit pharmaceuticals and HSI’s *Operation Stolen Promise*: an initiative targeting COVID-19 related fraud. Both training days included case studies from HSI Special Agents as well as presentations from private industry. Participants included Canadian law enforcement officers.
- Caribbean Regional Intellectual Property and Global Trade Enforcement Training – Punta Cana, Dominican Republic**
 On August 2-6, 2021, the IPR Center’s Global Trade Investigations Division – in collaboration with HSI Caribbean and HSI Santo Domingo – hosted the Caribbean Regional Intellectual Property Rights and Global Trade Enforcement Workshop. The workshop was attended by law enforcement, customs officials, and prosecutors from the Dominican Republic, Haiti, Jamaica, St. Kitts and Nevis, Guadeloupe, Aruba, Bahamas, Curacao, Trinidad and Tobago, Barbados, Turks and Caicos, Sint Maarten, the Cayman Islands, and the USVI. Remarks were provided by Acting Executive Associate Director Steve Francis and workshop topics were supported by HSI’s Intellectual Property Unit, Counter Proliferations Investigations Unit, Cyber Crime Center, and Trade Transparency Unit. Presentations were also provided by the Caribbean Community (CARICOM) and subject matter experts from CBP, FBI, Interpol, USPTO, and the U.S Department of Justice. Industry representatives from Pfizer, Colgate Palmolive, and Philip Morris International also delivered presentations on their enforcement efforts and their collaboration with law enforcement to combat illicit trade.

The training workshop addressed challenges and best practices related to interdiction, investigation, and prosecution of intellectual property and other trade-related crimes, as well as HSI and the USG’s support of partner law enforcement agencies in disrupting transnational criminal networks involved in these illicit activities. The workshop emphasized the importance of interagency coordination and international cooperation in ensuring successful enforcement and prosecution of IP and other trade-related crime in the region.

- Department of Justice, ICHIP Latin America Workshop on *Intellectual Property Rights and Criminal Process* – Virtual Webinar**
 On August 30 and September 1, 3, 6, 8, and 10, 2021, the Department of Justice’s International Computer Hacking and Intellectual Property (ICHIP) Advisor for Latin America and the Caribbean hosted a virtual workshop on *Intellectual Property Rights and Criminal Process*. The program was coordinated between the ICHIP and the School of the Judicial Branch of Panama, for Judges and Appeal Judges (Magistrates in Panama) from the Criminal Branch in Panama. The program provided participants an overview of the IPR criminal process, all the concepts behind it, and case studies. HSI supported the workshop on days 1 and 3, with speakers presenting on the topic of *Investigations of*

Crimes Against Intellectual Property Rights in the U.S. with investigative case-study examples.

- **Combatting Pharmaceutical Crime in the Post COVID Era, APAC Region – Virtual Webinar**
On September 7, 2021, HSI Singapore – along with representatives from Pharmaceutical Security Institute (PSI), Interpol, Moderna, and the International Trademark Association (INTA) – conducted a virtual workshop on combatting pharmaceutical crime in the post-COVID era. The workshop was attended by over 40 law enforcement agencies and pharmaceutical representatives from the APAC region. HSI Singapore provided an overview of HSI Operations and shared HSI's global efforts in combatting COVID-19 related fraud through *Operation Stolen Promise*. HSI Singapore highlighted the strategic multi-pronged approach of *Operation Stolen Promise* and the importance of public private partnership and intelligence sharing amongst international law enforcement agencies to combat fraudulent activities.
- **COVID-19 Fraud Typology Training – Indonesia – Virtual Webinar**
On September 7, 2021, HSI Jakarta – along with representatives from Pfizer – conducted a joint virtual training for Indonesian Customs and Excise (Customs), Indonesian National Police (INP), and the National Agency for Drug and Food Control of Indonesia (BPOM). During the virtual training session, HSI Jakarta provided an overview of HSI Operations, and shared HSI's global efforts in combatting COVID-19 related fraud through Operation Stolen Promise. HSI Jakarta also provided examples of health related, cyber related, financial related, and imposter related COVID-19 Fraud Typologies encountered by HSI along with several case examples of adjudicated HSI investigations. Pfizer Global Security provided training related to the proper labeling, transportation, and storage of its COVID-19 vaccine. Pfizer also discussed various COVID-19 vaccine frauds they have encountered along with red-flag indicators of such illicit activity. A total of 118 seminar attendees participated from Customs, INP, and BPOM (who represented various regional units throughout Indonesia). The training helped strengthen awareness of COVID-19 Fraud Typologies and solidified ties between Bi-Mission Indonesia/HSI Jakarta, Customs, INP, and BPOM.
- **U.S.-Singapore Third Country Training Program (TCTP) on *Challenges and Strategies for Protecting and Enforcing IP in the Digital Economy* – Virtual Webinar**
On September 30, 2021, HSI Singapore participated in a virtual intellectual property event on *Challenges and Strategies for Protecting and Enforcing IP in the Digital Economy* for the U.S.-Singapore Third Country Training Program (TCTP). The TCTP is a partnership between the Singapore Ministry of Foreign Affairs and the U.S. Department of State which jointly conducts capacity building courses for Southeast Asian countries. The U.S. and Singaporean governments cooperatively design and implement the training courses, which feature technical experts and trainers from both countries. HSI Singapore participated in a panel discussion highlighting HSI efforts in enforcing IP crime, including an overview of the IPR Center and Operation In Our Sites. The webinar was attended by governmental representatives from countries throughout Southeast Asia

(including Brunei, Cambodia, Thailand, Myanmar, Indonesia, Laos, Malaysia, Philippines, Timor-Leste, Vietnam) and the ASEAN Secretariat.

- **CBP Asia Pacific Economic Cooperation (APEC) Sub-Committee on Customs Procedures (SCCP)**

In early FY 2021, CBP led the Counterfeit COVID-19 Products Operation for the APEC SCCP, which was a voluntary mutual enforcement operation that included eight economies and focused on counterfeit COVID-19 items. The eight participating economies (Australia, Japan, Mexico, New Zealand, Papua New Guinea, Peru, Thailand, and the U.S.) shared their operation results and practices for IPR enforcement using the template created by CBP. Along with providing the seizure statistics for the operation, economies provided information on their methods for screening and targeting shipments; their use of risk management to identify potentially infringing shipments; their ability to make seizures and assess penalties and fines; the resources they dedicate to IPR enforcement; their collaboration with rightsholders; and recent trends they have seen regarding counterfeit items. This operation shed light on best practices for interdicting counterfeit goods and provided an information-sharing opportunity. CBP presented results of the effort at the February 2021 APEC SCCP meeting in New Zealand.

In June 2021, CBP conducted another Counterfeit COVID-19 Products Operation, which focused on bilateral relations and information sharing with the economy of Peru. The operation allowed Peru and the US to assess IPR trends since the previous operation. Both presented their results to the APEC SCCP at the virtual meeting held in August.

DEPARTMENT OF JUSTICE

DEPARTMENT OF JUSTICE

Department of Justice (DOJ) Appendix for FY 2021 Annual Report

This appendix for the Department of Justice (DOJ) is in two parts. The first part is based on DOJ's report to Congress for FY 2020 under Section 404 of the PRO IP Act. The second part discusses the Department's activities during FY 2021 relating to intellectual property protection and enforcement.

I. The Justice Department's report to Congress for FY 2020 under the PRO IP Act.

The Department of Justice (the "Department" or "DOJ") submits an annual report to 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 following is the Pro IP Act Annual Report for FY 2020 reproduced in its entirety. The Pro IP 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").

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 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 ongoing, 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 investigating 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 2020.⁵ 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.

⁵ 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.”

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 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.⁶

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.

⁶ 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/ip/f/pro-ip-act-reports>. The Department’s FY 2010–FY 2019 PRO IP Reports are available at the same location.

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 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.⁷ 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

⁷ 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.

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.⁸ 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.⁹ These activities have included training investigators and

⁸ 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.

⁹ 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

prosecutors in the investigation and prosecution of IP crimes; contributing to the Office of the United States Trade Representative's Special 301 process of evaluating the adequacy of our trading partners' criminal IP laws and enforcement regimes; helping to catalogue and review the United States government's IP training programs abroad; and implementing an aggressive international program to promote cooperative enforcement efforts with our trading partners and to improve substantive laws and enforcement regimes in other countries.

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

The Department achieved notable success in FY 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

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.

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 Chauffeur. 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 Chauffeur 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 Chauffeur. 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 Bridi 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.

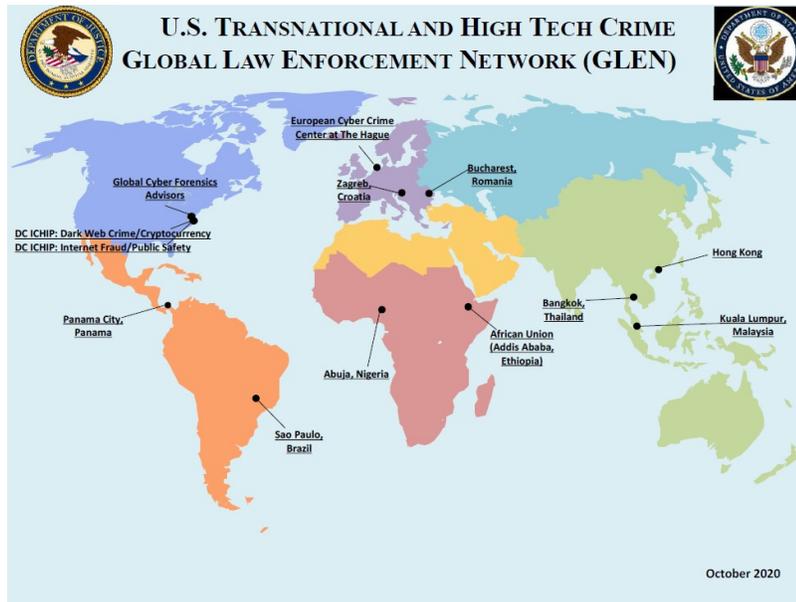
International Outreach and Training

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.¹⁰

¹⁰ 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

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.

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 Attorney Advisor, 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 General 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 Lanka 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 Combating 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 recommended that Romania 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 2020.¹¹

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.

¹¹ This portion of the DOJ appendix is the FY20 Pro-IP Act Report reproduced in its entirety. For additional context, Romania submitted its edits to the work plan to Washington in March 2021. After receiving minor edits back in September 2021, it has not yet formally approved the new version of the work plan, although Romania has already started implementing provisions of the document's initial draft, including appointing a high-level coordinator.

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 Pharmacime 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/iprf> 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.¹² 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.

¹² 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.

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.¹³

Charge	Cases charged	Percentage
Trademark <i>Trafficking in counterfeit goods, 18 U.S.C. § 2320</i>	23	61%
Copyright <i>Criminal copyright infringement, 17 U.S.C. § 506; 18 U.S.C. § 2319</i>	4	10%
<i>Counterfeit labels, 18 U.S.C. § 2318</i>	0	0%
<i>DMCA, 17 U.S.C. § 1201</i>	3	8%
Economic Espionage Act <i>Economic espionage, 18 U.S.C. § 1831 Theft of trade secrets, 18 U.S.C. § 1832</i>	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

¹³ 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.

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.

* * *

II. The following is a discussion of Department of Justice (DOJ) activities relating to intellectual property (IP) protection and enforcement, including litigation activities in which arrests, charges, indictments, guilty pleas or verdicts, and/or sentencing took place during FY 2021.

In addition to the litigation activities discussed below, DOJ also engages in IP protection and enforcement through other activities, many of which involve collaboration with other Federal agencies. Examples of these interagency collaborations during FY 2021 are discussed in the other appendices to this report.

For example, the appendix for the State Department discusses the Global Law Enforcement Network (GLEN) of DOJ attorneys – known as International Computer Hacking and Intellectual Property (ICHIP) advisors – who are posted around the world and are primarily funded by the State Department. The ICHIPs train and mentor their foreign law enforcement counterparts; collaborate with USG offices in the region (e.g., US embassy staff, IP Counselors and Attachés, HSI Attachés, and FDA and CBP personnel); and engage with IP rightsholders and other non-governmental stakeholders. The FY 2021 activities of the various ICHIPS are discussed elsewhere in this report, including in the appendices for the Department of Commerce, Homeland Security, and State.

INTELLECTUAL PROPERTY CASES FY 2021

COPYRIGHT / PRE-RELEASE / CAMCORDING / COUNTERFEIT LABELS (17 U.S.C. § 506, 18 U.S.C. §§ 2319, 2318)

- ***NJ, NY, CA Defendants Indicted for Nationwide Copyrighted IPTV Theft Scheme.*** On September 22, 2021, Bill Omar Carrasquillo of Swedesboro, NJ; Jesse Gonzales of Pico Rivera, CA; and Michael Barone of Richmond Hill, NY, 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. (EDPA, FBI, IRS)
<https://www.justice.gov/usao-edpa/pr/nj-ny-ca-defendants-indicted-nationwide-copyrighted-iptv-theft-scheme>
- ***Three Employees of a Long Island Information Technology Company Plead Guilty to Criminal Copyright Infringement.*** On September 15, 2021, Michael Calabria, Joseph Keegan, and Casey Silver pleaded guilty to criminal copyright infringement. Calabria and Keegan were principals of Constructure Technologies, LLC (“Constructure”), located in Melville, New York, and Silver was a Constructure employee. The charge relates to the

defendants' installing unlicensed versions of software by using "cracking" programs or "key generators," which allowed Constructure employees to activate copies of the software without paying for a license and obtaining a key. In addition to the guilty pleas, Constructure itself was charged with a felony violation of the Digital Millennium Copyright Act ("DMCA") and agreed to pay a \$60,000 fine.

According to court filings, Constructure provided information technology services, helping install, manage and service various networks and other technology products for small and medium sized businesses. Calabria was Constructure's President, Keegan was the Chief Technology Officer, and Silver was a Project Manager. Between 2011 and 2018, Constructure sold, installed and provided services for computer programs that were copyrighted and then sold by software companies ("Victim Software Companies"), including VMWare, a global cloud computing software company. Some of those computer programs were designed so that they could not be activated until a user paid the company for a "license" to use that software. In purchasing a license, the user received a "key"—a string of letters, numbers and symbols—that, when entered into the copy of software obtained by the user, activated the software. Constructure's clients generally paid Constructure to purchase licenses for such computer programs and to activate those programs with a legitimate license key.

Starting in or about 2011, Calabria, Keegan, and Silver helped to operate Constructure's business in part by installing unlicensed versions of software from Victim Software Companies by using cracking programs or key generators, which allowed Constructure to activate copies of the software without paying for a license and obtaining a key. Constructure employees, often at the express direction of Calabria or Keegan, used cracking programs or key generators to install software from multiple Victim Software Companies.

Constructure employees, including Keegan, obtained license keys and cracking programs from the internet. They also tested those programs on a computer server located in the basement of Constructure's office in Melville and on a file-sharing site controlled by Constructure, so that the programs could be used remotely by Constructure employees. By installing working, but unlicensed, versions of software, Constructure was able to bill a customer for the software, under the pretense that Constructure purchased a copy on behalf of the customer, while not actually paying for it. Constructure employees did not inform Constructure's clients or the Victim Software Companies that Constructure employees used "cracks" to install those programs. From approximately 2011 to approximately 2018, Constructure employees installed cracked software programs for multiple clients, including clients located in Hicksville, New York; Mineola, New York; Manhattan, New York; and Bridgewater, New Jersey. (EDNY, New York Cybercrime Task Force, FBI) <https://www.justice.gov/usao-edny/pr/three-employees-long-island-information-technology-company-plead-guilty-criminal>

- ***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. On August 26, 2020, the indictments were unsealed charging Umar Ahmad, George Bridi, and Jonatan Correa with copyright infringement. Bridi's indictment also included wire fraud for involvement in the Sparks Group, an international piracy group involved in illegally distributing movies and television shows on the internet, and conspiracy to transport stolen property interstate. Co-defendant Jonatan Correa, a/k/a "Raid," previously pled 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.

According to the allegations contained in the Indictments, from 2011 onward, Ahmad, Bridi, Correa, and others known and unknown, were members of the Sparks Group. In furtherance of its scheme, 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 thereafter uploaded copies of the copyrighted content onto servers controlled by the Sparks Group, where 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 Bridi arranged for discs to be picked up, mailed, or 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 further distribution on the internet. The Sparks Group has caused tens of millions of dollars in losses to film production studios. (SDNY, DHS-HSI, USPIS, OIA)

<https://www.justice.gov/usao-sdny/pr/acting-us-attorney-announces-federal-charges-and-international-operation-dismantle-0>

<https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-extradition-british-national-participation-online-film>

- ***Newport Man Sentenced to Federal Prison for Creating Illegal Video Streaming and Downloading Websites.*** On July 9, 2021, Talon White, 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. The content included movies that had yet to be released to the public. In total, White's scheme netted more than \$8 million. While operating the scheme, White also underreported his income by more than \$4.4 million, willfully evading the payment of more than \$1.9 million in taxes owed from 2013 through 2017. As part of the plea agreement, White has 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. It is anticipated these forfeited assets will be applied to White's restitution obligations. (DOR, HSI, IRS-CI)

<https://www.justice.gov/usao-or/pr/newport-man-pleads-guilty-copyright-infringement-creating-illegal-video-streaming-and>

<https://www.justice.gov/usao-or/pr/newport-man-sentenced-federal-prison-creating-illegal-video-streaming-and-downloading>

- ***Bowie Man Sentenced to 12 Months and One Day in Federal Prison for Selling More Than \$300,000 Worth of Counterfeit DVDs.*** On May 24, 2021, Olayinka Wahab of Bowie, Maryland, was sentenced to 12 months and one day in federal prison, followed by three years of supervised release, for copyright infringement in connection with his sale of counterfeit DVDs containing copyrighted works, including popular movies, television shows, and fitness programs. Wahab was also ordered to pay \$241,370.58 in forfeiture and \$165,961.53 in restitution to the victims of his copyright infringement. According to his plea agreement, between March 2009 and May 2018, Wahab sold approximately 18,306 DVDs or DVD sets, with a total retail value of \$315,761.44. Wahab knowingly sold counterfeit DVDs containing copyrighted works belonging to a number of production companies. In 2017, representatives from the Motion Picture Association (MPA) identified a seller on an internet marketplace offering DVD movies for sale at a discount. MPA purchased an item and analyzed the DVD upon receipt. The packaging and labeling were substantially indistinguishable from the packaging and labeling found on legitimate copies of the movie. The MPA was able to determine that the movie was counterfeit. Records obtained from the internet marketplace revealed that this seller had made over 10,000 sales of DVD or Blu-Ray discs of popular movies, television shows, or fitness programs between August 2016 and April 2018. Law enforcement officers, operating in an undercover capacity, subsequently conducted purchases from the seller. The DVDs purchased by the undercover officers were provided to MPA representatives for authentication and were determined to be counterfeit. Law enforcement determined that Wahab was the individual selling the counterfeit items. (DMD, HSI)
<https://www.justice.gov/usao-md/pr/bowie-man-pleads-guilty-copyright-infringement-selling-more-300000-worth-counterfeit-dvds>

<https://www.justice.gov/usao-md/pr/bowie-man-sentenced-12-months-and-one-day-federal-prison-selling-more-300000-worth>

- ***Former Video Store Owner Sentenced to Five Years for Selling Counterfeit DVDs.*** On December 22, 2020, Douglas Gordon was sentenced to five years in prison and two years of supervised release for mail fraud and copyright infringement stemming from his online sales of counterfeit DVDs. He was also ordered to pay restitution to victims defrauded in the scheme. A jury found Gordon guilty on October 29, 2019, after a seven-day 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 in 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 U.S. Immigration and Customs Enforcement's Homeland Security Investigations (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. (DME, HSI, USPIS, State/Local LE)
<https://www.justice.gov/usao-me/pr/federal-jury-convicts-former-video-store-owner-selling-counterfeit-dvds>
<https://www.justice.gov/usao-me/pr/former-video-store-owner-sentenced-five-years-selling-counterfeit-dvds>
- ***Bucksport Woman Sentenced for Aiding and Abetting Counterfeit DVD Scheme.*** On November 2, 2020, Heidi Pugliese of Bucksport, Maine was sentenced in federal court for aiding and abetting a mail fraud scheme. Pugliese was sentenced to five years of probation and was ordered to pay restitution to victims defrauded in the scheme. Pugliese pleaded guilty in August 2019 to aiding and abetting Douglas Gordon in carrying out his Maine-based scheme to sell counterfeit DVDs online. Gordon, the former owner of a chain of video rental stores in eastern Maine, operated three websites from which he made hundreds of thousands of dollars in sales of more than 48,000 counterfeit copies of copyright-protected movies. Pugliese assisted the scheme over a 21-month period from 2013 to 2015, during which time it brought in approximately \$140,000. Gordon was convicted of mail fraud and copyright infringement charges in October 2019 after a seven-day jury trial in which Pugliese testified for the government (Gordon's case is the prior item). (DME, USPIS, HSI, BBB)
<https://www.justice.gov/usao-me/pr/bucksport-woman-sentenced-aiding-and-abetting-counterfeit-dvd-scheme-0>

DIGITAL MILLENNIUM COPYRIGHT ACT (17 U.S.C. §§ 1201, 1204)

- ***Three Members of Notorious Videogame Piracy Group “Team Xecuter” Charged.*** On October 2, 2020, Max Louarn, a French national, Yuanning Chen, a Chinese national, and Gary Bowser, a Canadian national, were taken into custody and charged. Each defendant is 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. The enterprise targeted popular consoles, such as the Nintendo Switch, the Nintendo 3DS, the Nintendo Entertainment System Classic Edition, the Sony PlayStation Classic, and the Microsoft Xbox. According to court documents, the Team Xecuter criminal enterprise is comprised of over a dozen individual members located around the world, including developers who exploit vulnerabilities in videogame consoles and design circumvention devices; website designers who create the various websites that promote the enterprise’s devices; suppliers who manufacture the devices; and resellers around the world who sell and distribute the devices. The indictment alleges that due, to the illegal nature of its business, Team Xecuter continuously sought to evade enforcement efforts by victim companies, financial institutions, and law enforcement. Notably, Team Xecuter attempted to protect its overall business by using a wide variety of brands, websites, and distribution channels, according to the indictment.

From approximately June 2013 through August 2020, Team Xecuter used a variety of product names for its devices, such as the Gateway 3DS, the Stargate, the TrueBlue Mini, the Classic2Magic, and the SX line of devices that included the SX OS, the SX Pro, the SX Lite, and the SX Core. To support their illegal activity, Team Xecuter allegedly helped create and support online libraries of pirated videogames for its customers, and several of the enterprise’s devices came preloaded with numerous pirated videogames. According to the indictment, Team Xecuter even required customers to purchase a “license” to unlock the full features of its custom firmware, the SX OS, in order to enable the ability to play pirated videogames. In September 2020, Louarn and Bowser were arrested abroad in connection with the charges in this case. The United States will seek Louarn’s extradition to stand trial in the United States. Bowser was arrested and deported from the Dominican Republic, and appeared on October 2, 2020, in federal court. (WDWA, FBI, HSI, OIA)
<https://www.justice.gov/opa/pr/two-members-notorious-videogame-piracy-group-team-xecuter-custody>

TRAFFICKING IN COUNTERFEIT GOODS (18 U.S.C. § 2320)

- ***Florida Man Sentenced for Selling Counterfeit Drugs on the Dark Net.*** On August 24, 2021, Benjamin Burdick 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. Between June 2019 and August 2020, undercover federal agents purchased multiple packages of counterfeit pills from Burdick. When his home was searched pursuant to a federal search warrant in October 2020, agents recovered 16,000 counterfeit pills, a pill press, and almost \$150,000 in cash. (EDVA, FBI, USPIS, FDA, CPB) <https://www.justice.gov/usao-edva/pr/florida-man-sentenced-selling-counterfeit-drugs-dark-net>

- ***Four 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 a counterfeit goods scheme 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. Four defendants – Hai Long Zhou, Saiyin Hou, Yan Xue Huang (also known as “Yan Xue Zhou” and “Yan Xue Li Ming”), and Jian Fen Yang – were arraigned and each was released on a \$200,000 bond. Three additional defendants remain at large. As alleged in the indictment, between October 2019 and July 2021, the defendants participated in an international scheme to traffic counterfeit goods. The defendants first imported the goods in generic form from China into the Port of New York and New Jersey. The goods were then delivered to workshops and storage facilities controlled by some of the defendants in Queens and on Long Island. In those workshops, insignias, emblems, trademarks, and other brand signifiers were applied to the generic goods, converting them into purported brand name merchandise. These counterfeit goods were then sold as a part of the scheme directly to consumers and to wholesale buyers. The estimated retail value of the counterfeit-branded goods, had they been genuine, was in excess of \$130 million. (EDNY)

<https://www.justice.gov/usao-edny/pr/four-defendants-arrested-multimillion-dollar-counterfeit-goods-trafficking-scheme>

- ***Man Pleads Guilty to Selling Counterfeit Vapes.*** On April 29, 2021, Christopher Andrew Reyes of The Colony, Texas, pleaded guilty to conspiracy to import drug paraphernalia, specifically to selling counterfeit vape pens imported from China. According to court documents, Mr. Reyes admitted that he allowed employees of a vaping shop on Harry Hines Boulevard to order counterfeit THC vaping products online using his bank card. In September 2019, U.S. Customs & Border Protection agents intercepted a shipment of 2,400 counterfeit THC vaping devices addressed to Mr. Reyes and bound for his home. The vaping devices, which were sent from China and routed through DFW International Airport, bore the counterfeit trademark of a popular THC vape brand, “Cookies.” Agents estimated that at least five additional shipments of vaping products had been sent to Mr. Reyes. In plea papers, the defendant admitted that, after receiving the packages, he sold the contents back to the vaping shop for profit. His bank statements, which show large purchases from Chinese e-commerce company Alibaba (an online retailer similar to Amazon), backed up his admissions. (HSI, FDA, CBP, NDTX)

<https://www.justice.gov/usao-ndtx/pr/man-pleads-guilty-selling-counterfeit-vapes>

- Lebanon County Man Sentenced to Seventy Months' Imprisonment for Trafficking Counterfeit Drugs.*** On April 15, 2021, Stefan Knoche of Lebanon, Pennsylvania, was sentenced to 70 months' imprisonment 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. (MDPA, USPIS, FDA, DHS, HSI)
<https://www.justice.gov/usao-mdpa/pr/lebanon-county-man-charged-trafficking-counterfeit-drugs>
<https://www.justice.gov/usao-mdpa/pr/lebanon-county-man-sentenced-seventy-months-imprisonment-trafficking-counterfeit-drugs>
- Manufacturer Sentenced for Conspiring to Manufacture and Sell Counterfeit Goods.*** On April 12, 2021, Bernard Klein, a 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, 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 U.S. military.

According to court documents, Klein was sent samples of genuine clothing, apparel, and gear by Kohanbash to be reproduced. Prior to the approval of mass production of the counterfeit goods, Klein emailed photographs of the goods, as well as hangtags and labels, to Kohanbash for approval. After making any changes ordered by Kohanbash, 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 in order to avoid problems when shipments were inspected by U.S. Customs.

On June 13, 2019, Kohanbash pleaded guilty to conspiracy to commit wire fraud and trafficking in counterfeit goods and 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. (DRI, GSA, HSI, DCIS, CBP, Army-CID, AF-OSI)
<https://www.justice.gov/usao-ri/pr/manufacturing-broker-pleads-guilty-conspiracy-manufacture-and-sell-counterfeit-goods>
<https://www.justice.gov/usao-ri/pr/manufacturer-sentenced-conspiring-manufacture-and-sell-counterfeit-goods>

- ***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., and his spouse, Guojiao “Becky” Zhang, 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 plea agreements, Thompson Jr. was an Information Programs Officer employed by the Department of State at the U.S. Embassy in Seoul, a position that required him to maintain a security clearance. Zhang is married to Thompson Jr. and resided with him in Seoul. On December 18, 2019, Thompson and Zhang were arrested for their role in an international conspiracy to traffic in counterfeit goods from the U.S. Embassy in Seoul. 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 U.S. Thompson Jr. 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 Oregon. Thompson Jr. and Zhang also directed a co-conspirator in Oregon to ship items to purchasers across the U.S. (DOR, OIA, HRSP, CCIPS, USPIS)

<https://www.justice.gov/opa/pr/state-department-employee-and-spouse-indicted-trafficking-counterfeit-goods-us-embassy>

<https://www.justice.gov/opa/pr/state-department-employee-and-spouse-plead-guilty-trafficking-counterfeit-goods-us-embassy>

<https://www.justice.gov/opa/pr/former-state-department-employee-sentenced-prison-trafficking-counterfeit-goods-us-embassy>

- ***Georgia couple sentenced for importing and distributing male enhancement products and counterfeit goods from China as well as naturalization fraud.*** On February 24, 2021, Irfanali Momin and Shiba I. Momin a/k/a Saguftabanu Momin, husband and wife, 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. The Momins have also been criminally denaturalized as result of their convictions for naturalization fraud. According to the prosecution, the charges and other information presented in court, the Momins ordered and sold male enhancement products from China marketed under names such as “Black Ant King,” “Bull,” “Rhino 7,” and “Black Mamba” between August 2014 and November 2018. 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. (FDA, HSI, FBI)
<https://www.justice.gov/usao-ndga/pr/husband-and-wife-plead-guilty-naturalization-fraud-and-conspiring-illegally-import-and>
<https://www.justice.gov/usao-ndga/pr/georgia-couple-sentenced-importing-and-distributing-male-enhancement-products-and>

TRADE SECRET THEFT (18 U.S.C. § 1832)

- ***Engineer Ends Trial by Pleading Guilty to the Federal Crime of Conspiring to Steal Trade Secrets.*** On September 29, 2021, Gilbert Basaldua of Hilton Head, S.C., pleaded guilty to Conspiracy to Steal Trade Secrets from aircraft companies and Interstate Transportation of Stolen Property during the second day of his jury trial. Basaldua faces a statutory sentence of up to 10 years in prison on each charge, plus substantial financial penalties. 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 in the Southern District of Georgia 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. The conspirators intended to use the stolen information to quicken the process of obtaining Federal Aviation Administration certification for another company's product. (SDGA, FBI)
<https://www.justice.gov/usao-sdga/pr/three-indicted-conspiracy-steal-trade-secrets-aircraft-companies>
<https://www.justice.gov/usao-sdga/pr/defendant-pleads-guilty-conspiracy-steal-trade-secrets-aircraft-manufacturers>
<https://www.justice.gov/usao-sdga/pr/engineer-ends-trial-pleading-guilty-federal-crime-conspiring-steal-trade-secrets>
- ***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 (also known as Rose Sweihorn Tong), 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 indictment, in 2012, Jordanov and Lin are alleged to have co-founded JHL Biotech, Inc., a biopharmaceutical start-up headquartered in Zhubei, Taiwan, with offices in Wuhan, China, and Rancho Santa Fe, Calif. JHL Biotech is now known as Eden Biologics, Inc. and Chime Biologics (Wuhan), Ltd. The indictment alleges that Jordanov and Lin, beginning as early as 2008, engaged in a fraudulent scheme to steal thousands of confidential and proprietary documents from Genentech that eventually helped JHL Biotech secretly accelerate its development and production of "biosimilars," or generic versions of Genentech biologics. Some of the confidential documents stolen from Genentech and obtained by Jordanov and Lin allegedly contained trade secrets.

The indictment alleges that, starting in 2009, Lin recruited an experienced and accomplished scientist then working at Genentech and her husband to work as a team to purloin confidential information from within Genentech. Beginning in 2013, Lin and Jordanov allegedly used confidential information from the husband and wife team and other sources to help JHL Biotech cut corners, reduce costs, solve problems, save time, and otherwise accelerate product development timelines, secretly using Genentech's high-quality, confidential, intellectual property. In 2014, Jordanov and Lin supervised and managed a so-called "conversion" project whereby JHL employees converted confidential Genentech standard operating procedures or "SOPs" into JHL Biotech SOPs. For example, JHL employees engaged in the wholesale cutting and pasting of logos from the confidential documents by simply cutting out Genentech logos and pasting in JHL Biotech logos to make the Genentech SOPs appear, falsely, to be JHL Biotech SOPs. JHL Biotech employees allegedly drafted approximately ninety (90) different SOPs using Genentech documents, many of which were confidential and proprietary. JHL Biotech employees maintained a spreadsheet in which they identified Genentech SOPs that JHL Biotech possessed and tracked the progress to convert these into JHL Biotech SOPs. The widespread use of the stolen Genentech SOPs allegedly saved JHL Biotech thousands of dollars.

To profit from the trove of stolen confidential, proprietary, and trade secret information, Jordanov and Lin, according to the indictment, then carried out a scheme to defraud JHL Biotech's potential investors and strategic partners. To induce investment, and obtain money for JHL Biotech and themselves, Jordanov and Lin allegedly defrauded investors by concealing the extent to which JHL Biotech used stolen intellectual property to start, accelerate, and conduct its business. The indictment alleges that, in late 2016, JHL Biotech entered a strategic partnership with Sanofi S.A., a French multinational pharmaceutical company headquartered in Paris, France, to manufacture and distribute biosimilars in China. As part of the agreement, in December 2016, Sanofi allegedly paid \$101 million to JHL Biotech, using foreign and interstate wires to carry out the corporate transaction. This cash payment allegedly was part of a strategic relationship worth potentially \$337 million to JHL Biotech. To induce Sanofi's payment of \$101 million in cash, Jordanov allegedly signed representations and warranties that falsely stated that JHL Biotech's knowledge, research, development, use, and manufacture of certain biosimilars had been conducted without infringing or misappropriating intellectual property from any third party. Jordanov also allegedly made false and misleading statements about consultants used by JHL Biotech and otherwise concealed from Sanofi the secret work of the Genentech insider for JHL Biotech. In 2019, following the public disclosure of some of the alleged criminal conduct, the value of JHL Biotech, once as high as approximately \$916 million, allegedly crashed. (DNCA, IRS, FBI)

<https://www.justice.gov/usao-ndca/pr/former-ceo-and-coo-jhl-biotech-charged-conspiracy-steal-trade-secrets-and-commit-wire>

<https://www.justice.gov/usao-ndca/pr/former-ceo-and-coo-jhl-biotech-convicted-conspiracy-steal-trade-secrets-and-commit-wire>

- Owners of Florida Teacher Certification Exam Preparation Company Plead Guilty to Racketeering Conspiracy and Conspiracy to Commit Theft of Trade Secrets.*** On August 10, 2021, Kathleen M. Jasper and Jeremy M. Jasper, both of Estero, Florida, pled guilty to racketeering (RICO) conspiracy and conspiracy to commit theft of trade secrets. Court documents reflect that, since January 2016, the Jaspers, who are both certified Florida teachers, stole content and conspired with others to steal content from the Florida Teacher Certification Exams (FTCE) and the Florida Educational Leadership Exam (FELE) and included the stolen content in the test preparation materials and services that were sold through their business, NavaEd, LLC (“NavaEd”), for personal profit. NavaEd, LLC, was a company that offered tutoring and training to prepare prospective Florida educators to successfully take and pass the FTCE and the FELE, which are required for certification in the state of Florida. NavaEd offered training publications for sale worldwide directly through its website and through third-party e-commerce websites, such as Amazon and Shopify. Both Kathleen and Jeremy Jasper took the FTCE and FELE multiple times – after having already passed the exams – in order see and memorize, or harvest, as many different exam questions as possible. The Jaspers also directed NavaEd employees and independent contractors to take the FTCE and FELE for the purpose of harvesting exam questions and answers. The Jaspers and NavaEd customers shared the stolen FTCE and FELE test content with each other through email, phone, video conferencing, and messaging applications. The Jaspers republished the stolen FTCE and FELE test content – verbatim and almost verbatim – into NavaEd publications that were written to prepare future Florida teachers and school administrators for the certification exams. These publications and other NavaEd FTCE and FELE preparation materials were disseminated and used during NavaEd training seminars and tutoring sessions. (DNFL, USDE, FL Dept. of Law Enforcement)
<https://www.justice.gov/usao-ndfl/pr/owners-florida-teacher-certification-exam-preparation-company-plead-guilty-racketeering>
- Bixby Man Pleads Guilty to Conspiracy to Steal Trade Secrets.*** On June 2, 2021, Joshua Decker of Bixby, Oklahoma, pleaded guilty to conspiracy to steal trade secrets from an oil and gas company. On May 26, 2021, the government filed a one-count Superseding Information charging Decker with conspiracy to steal, download, and possess trade secrets. According to the Superseding Information, Decker was a controller for the valve division of an oil and gas company that serves customers engaged in drilling and production. With its valve operations headquartered in Oklahoma City, the company manufactures compact manifold ball valves sold across the United States. In March 2017, while employed as the controller at the company, Decker registered with the Oklahoma Secretary of State a new company called Legacy Valve Systems (“Legacy”). He then recruited co-workers at the victim company to join him at Legacy. The Superseding Information alleges that from March to September 2017, Decker conspired to steal numerous trade secrets from the victim company. Specifically, it alleges that Decker and others acting at his direction downloaded the technical drawings, material specifications, and manufacturing instructions for the victim company’s valves, and Decker transmitted the victim company’s detailed financial information – including cost information and sales by product and customer – by email to himself. The Superseding Information further alleges that Decker provided the victim company’s drawings to an individual who copied them and replaced the victim company’s logo with a Legacy logo to begin manufacturing and selling valves to compete with the

victim company. Decker then allegedly directed others to delete all their text messages and files, including messages on an encrypted application, to conceal their theft from the victim company. At the June 2 hearing, Decker pleaded guilty to conspiracy to steal trade secrets. He admitted that the victim company undertook several measures to protect their information as trade secrets. Decker admitted that he, along with others, planned to take and use the drawings of the victim company's valves to create products for Legacy. He also admitted that he possessed many of the drawings on his own laptop and that he instructed those working with him to delete their communications about the drawings they took. (WDOK, FBI)

<https://www.justice.gov/usao-wdok/pr/bixby-man-pleads-guilty-conspiracy-steal-trade-secrets>

- ***Massachusetts Man Pleads Guilty To Attempting To Steal Trade Secrets From Nevada Defense Company.*** On May 24, 2021, Peter James Cariani of Boston, MA, pleaded guilty to attempting to steal trade secrets belonging to his employer, a Nevada-based defense contractor. According to court documents and admissions made in court, Cariani was employed as a systems engineer by Sierra Nevada Corporation (SNC). On April 7, 2015, without authority to do so, Cariani downloaded tens of thousands of electronic files from SNC's computer network. The files contained trade secret information related to SNC's Radar Enhanced Vision System: a unique onboard aircraft radar sensing system that displays digital images of the ground for pilots flying in zero-visibility conditions. Cariani transferred the files to a personal external hard drive, and later transmitted information derived from the files to others for potential economic benefit. When entering his guilty plea, Cariani admitted that he knowingly downloaded trade secret information from SNC's network and he knew his actions would harm SNC. An investigation was initiated by the FBI's Reno branch after SNC detected (and reported) that an unauthorized electronic device had been used to download files from its computer network. (DNV, FBI)
<https://www.justice.gov/usao-nv/pr/massachusetts-man-pleads-guilty-attempting-steal-trade-secrets-nevada-defense-company>
- ***Niskayuna Man Sentenced for Stealing GE's Trade Secrets.*** On April 30, 2021, Yang Sui of Niskayuna, New York, was sentenced to one year of probation, and to pay a \$5,000 fine, for stealing trade secrets. Sui pled guilty in May 2020, to stealing trade secrets belonging to the General Electric Company. As part of his 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. (NDNY, FBI, NSD)
<https://www.justice.gov/usao-ndny/pr/niskayuna-man-pleads-guilty-stealing-trade-secrets-ge>
<https://www.justice.gov/usao-ndny/pr/niskayuna-man-sentenced-stealing-ge-s-trade-secrets>
- ***Chinese Businessman Charged With Conspiring To Steal Trade Secrets.*** On February 25, 2021, Chi Lung Winsman Ng, aka Winsman Ng, a Chinese businessman residing in Hong Kong, was indicted for conspiring to steal General Electric's (GE) trade secrets involving the company's silicon carbide MOSFET technology worth millions of dollars. The indictment

alleges that, between about March 2017 and January 2018, Ng and at least one co-conspirator plotted to develop a business that would manufacture and sell silicon carbide MOSFETs using trade secrets stolen from GE. Ng conspired with at least one other person, a GE engineer of more than seven years, to steal MOSFET trade secrets and other proprietary information from GE. Ng and co-conspirator #1 allegedly used those trade secrets to create a business plan and develop PowerPoint presentations which they gave to prospective investors. Ng and co-conspirator #1 told potential investors that their business could be profitable within three years and that their start-up business possessed assets – tangible and intangible – they estimated to be worth \$100 million. As part of the scheme, they sought approximately \$30 million in funding in exchange for an ownership stake in their start-up company. In August 2017, Ng and co-conspirator #1 allegedly met in China and gave presentations to a Chinese investment company that was considering providing funding to Ng's start-up company. Ng has yet to be arrested. (NDNY, FBI, NSD)
<https://www.justice.gov/opa/pr/chinese-businessman-charged-conspiring-steal-trade-secrets>

- ***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, 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, 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.

Until recently, bisphenol-A (BPA) was used to coat the inside of cans and other food and beverage containers to help minimize flavor loss, and prevent the container from corroding or reacting with the food or beverage contained therein. However, due to the discovery of potential harmful effects of BPA, companies began searching for BPA-free alternatives. These alternatives are difficult and expensive to develop. From December 2012 through August 31, 2017, You was employed as Principal Engineer for Global Research by a company in Atlanta, which had agreements with numerous companies to conduct research and development, testing, analysis and review of various BPA-free technologies. Due to her extensive education and experience with BPA and BPA-free coating technologies, she was one of a limited number of employees with access to trade secrets belonging to the various owners. From approximately September 2017 through June 2018, You was employed as a packaging application development manager for a company in Kingsport, Tennessee, where she was one of a limited number of employees with access to trade secrets belonging to that company.

The indictment alleges that You, Liu, and a third co-conspirator formulated a plan in which You would exploit her employment with the two American employers to steal trade secrets and provide the information, for the economic benefit of trade secrets, to the Chinese

company that Liu managed, which would manufacture and profit from products developed using the stolen trade secrets. In exchange, Liu would cause the Chinese company to reward You for her theft, by helping her receive the Thousand Talent and another financial award, based on the trade secrets she stole, and by giving You an ownership share of a new company that would “own” the stolen trade secrets in China. The conspirators also agreed to compete with U.S. and foreign companies, including some of the owners of the stolen trade secrets, in China and elsewhere, by selling products designed, developed and manufactured using the stolen trade secrets. (EDTN, NSD-CES, FBI)

<https://www.justice.gov/opa/pr/one-american-and-one-chinese-national-indicted-tennessee-conspiracy-commit-theft-trade>

<https://www.justice.gov/usao-edtn/pr/one-chinese-national-and-one-american-indicted-east-tennessee-conspiracy-commit-theft>

<https://www.justice.gov/opa/pr/phd-chemist-convicted-conspiracy-steal-trade-secrets-economic-espionage-theft-trade-secrets>

- ***Hospital Researcher Sentenced to Prison for Conspiring to Steal Trade Secrets and Sell to China.*** On April 19, 2021, Yu Zhou 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, 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 2021 to 30 months in prison for her role in the scheme (Chen’s case is the next item).

Court documents detail that Zhou and Chen conspired to steal and then monetize one of the trade secrets by creating and selling exosome “isolation kits.” Zhou’s research at Nationwide Children’s included a novel isolation method in which exosomes could be isolated from samples as small as one drop of blood. This method was vital to the research being conducted in Zhou’s lab focused on necrotizing enterocolitis – a condition found primarily in premature babies – from whom only small amounts of fluid can safely be taken. Zhou and Chen started a company in China to sell the kits. The defendants received benefits from the Chinese government, including the State Administration of Foreign Expert Affairs and the National Natural Science Foundation of China. Zhou and Chen were also part of application processes related to multiple Chinese government programs, including talent plans, used by the Chinese government to transfer foreign research and technology to the Chinese government. (SDOH, NSD, FBI)

<https://www.justice.gov/opa/pr/couple-who-worked-local-research-institute-10-years-charged-stealing-trade-secrets-wire-fraud>

<https://www.justice.gov/opa/pr/hospital-researcher-sentenced-prison-conspiring-steal-trade-secrets-and-sell-china>

- Hospital Researcher Sentenced to Prison for Conspiring to Steal Trade Secrets, Sell Them in China.*** On February 1, 2021, Lee Chen, formerly of Dublin, Ohio, was sentenced to 30 months in prison for conspiring to steal exosome-related trade secrets concerning the research, identification, and treatment of a range of pediatric medical conditions. Chen pleaded guilty on July 30, 2020, when she 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 and her husband, alleged co-conspirator Yu Zhou, 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 were charged with conspiring to steal at least five trade secrets related to exosome research from Nationwide Children’s Hospital. 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. Chen will forfeit approximately \$1.25 million, 500,000 shares of common stock of Avalon GloboCare Corp. and 400 shares of common stock of GenExosome Technologies Inc. As part of her sentence, she was ordered to pay \$2.6 million in restitution. Chen and Zhou were arrested in California in July 2019. (SDOH, NSD, FBI)

<https://www.justice.gov/opa/pr/couple-who-worked-local-research-institute-10-years-charged-stealing-trade-secrets-wire-fraud>

<https://www.justice.gov/opa/pr/researcher-pleaded-guilty-conspiring-steal-scientific-trade-secrets-ohio-children-s-hospital>

<https://www.justice.gov/opa/pr/hospital-researcher-sentenced-prison-conspiring-steal-trade-secrets-sell-them-china>
- Researcher Charged with Theft of Trade Secrets from New Jersey-Based Pharmaceutical Company.*** On January 13, 2021, Shafat A. Quadri of North Potomac, Maryland, was arrested on charges of stealing and illegally transmitting trade secrets. According to the documents filed in this case and statements made in court, “Company 1” is based in New Jersey and is one of the largest pharmaceutical companies in the world, creating vaccines, medicines and consumer healthcare products. In October 2019, Company 1 contacted the FBI to report suspicious activity by Quadri, who had been employed there since 2015 as director of medical and scientific affairs, immune oncology. Quadri had access to sensitive intellectual property of the company, including research and other trade secrets. He remained at the company through Sept. 30, 2019. Company 1 reported that an internal investigation revealed that, before he left in September 2019, Quadri copied and removed thousands of files containing Company 1’s proprietary information, including research protocols, compound data, and strategic plans. Quadri used unauthorized USB devices and personal email accounts to copy, transfer, and retain proprietary information from Company 1. Some documents that were copied and removed were outside of Quadri’s area of work responsibility. Quadri was not authorized to keep or transfer any sensitive or proprietary documents. (DNJ, FBI)

<https://www.justice.gov/usao-nj/pr/researcher-charged-theft-trade-secrets-new-jersey-based-pharmaceutical-company>

- Chinese Energy Company, U.S. Oil & Gas Affiliate and Chinese National Indicted for Theft of Trade Secrets.*** On October 29, 2020, a federal grand jury returned an indictment alleging corporate entities conspired to steal technology from a Houston-area oil & gas manufacturer. Jason Energy Technologies Co. (JET) in Yantai, People's Republic of China; Jason Oil and Gas Equipment LLC (JOG) USA; and Chinese national Lei Gao, aka Jason Gao, are charged with conspiracy, theft of trade secrets and attempted theft of trade secrets. Also charged in relation to the case is Robert Erford Jr. of Dayton, Texas, who worked for a Houston-area company and previously pleaded guilty to conspiracy to commit trade secrets. On or about November 7, 2019, Gao allegedly met with Erford at the JOG offices located in Houston. According to the indictment, Erford signed a consultancy agreement that Gao provided at that time, indicating Erford would work in China as a consultant to assist JOG in coiled tubing technology. At that meeting, Erford was also provided a letter from the JET general manager inviting him to visit in order to have a technical exchange and discussion, according to the charges. That letter allegedly indicated a goal of helping to promote the company's manufacturing efficiency, reduce machine failure, and increase production capacity. Without authorization, on or about November 22, 2019, Erford allegedly transferred a victim company document that contained a trade secret from the U.S. to China for JET's benefit. The indictment further alleges that from approximately November 25-29, 2019, Erford held meetings with Gao and JET officials at JET's offices in China and its coiled tubing facilities. At those meetings, they allegedly discussed coiled tubing technology, including victim company proprietary technology, practices and procedures. The charges also allege authorities obtained evidence that Erford and Gao used encrypted messaging app WeChat in December 2019 to obtain, collect, and copy victim company manufacturing information. (SDTX, FBI, NSD)
<https://www.justice.gov/opa/pr/chinese-energy-company-us-oil-gas-affiliate-and-chinese-national-indicted-theft-trade-secrets>
- 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.

UMC pleaded guilty to a superseding information charging the company with one count of criminal trade secret theft in violation of 18 U.S.C. § 1832(a)(3). The other criminal charges and a parallel civil suit by the United States against UMC will be dismissed. The criminal prosecution of Fujian Jinhua and the three individual defendants will continue, as will a civil

action seeking to enjoin Fujian Jinhua from the further transfer of stolen trade secrets and the export to the U.S. of products manufactured by Fujian Jinhua that were made using the stolen trade secrets.

According to the facts admitted in connection with the guilty plea, UMC hired the three individual defendants – Chen Zhengkun, a.k.a. Stephen Chen; He Jianting, a.k.a. J.T. Ho; and Wang Yungming, a.k.a. Kenny Wang – from Micron’s Taiwan subsidiary. UMC made Chen a senior vice president and assigned him to lead negotiation of an agreement with Fujian Jinhua to develop Dynamic Random Access Memory (DRAM) technology for Fujian Jinhua. As a foundry company, UMC previously made logic chips designed by other companies but did not make DRAM memory chips. Chen hired Ho and Wang to join the DRAM development team, and Ho and Wang brought Micron’s confidential information to UMC from Micron’s Taiwan subsidiary. After UMC’s Information Technology Department found Micron’s intellectual property on Ho’s UMC computer, Chen approved the issuance of two “off network” laptop computers that allowed UMC employees to access Micron confidential information without further detection by UMC’s IT department. In particular, Wang used one file containing Micron’s trade secrets to adjust UMC’s design rules for the memory in question. Later, when Taiwan authorities searched UMC’s offices, Ho and Wang asked another UMC employee to hide papers, notes, USB drives, a personal phone, and a laptop computer while the Taiwan authorities executed their search warrants. Taiwan authorities recovered only one of the two off-network laptops. The hard drive of the other was reformatted and concealed from Taiwan authorities. Beginning in the month of the Taiwan raids, Chen became president of Fujian Jinhua and took charge of its memory production facility. (NDCA, FBI, NSD)

<https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage>

<https://www.justice.gov/opa/pr/taiwan-company-pleads-guilty-trade-secret-theft-criminal-case-involving-prc-state-owned>

- ***Lexington Couple and their Semiconductor Company Indicted on Charges of Theft of Trade Secrets from Norwood Semiconductor Company.*** On October 1, 2020, Haoyang Yu, a/k/a “Jack Yu,” a/k/a “Harry Yu,” a/k/a “Jack Tricon,” of Lexington, MA, and his company, Tricon MMIC LLC (Tricon), were charged in a 24-count superseding indictment in connection with the theft of hundreds of files containing proprietary information from Analog Devices, Inc. (ADI), a worldwide semiconductor company headquartered in Norwood. The charges included three counts of possession and attempted possession of a trade secret; two counts of smuggling; two counts of transporting stolen goods; one count of visa fraud; and one count of procuring U.S. citizenship unlawfully. Yu and his wife, Yanzhi Chen, also of Lexington, were also charged with three counts of wire fraud and aiding and abetting wire fraud. Yu was previously charged by indictment in June 2019 with stealing, copying, downloading, and possessing ADI’s trade secrets. It is alleged that, while working for ADI, Yu downloaded hundreds of highly confidential schematic design and modeling files that belonged to ADI, and uploaded many of these files to his personal Google drive account. The files YU stole from ADI were worth millions of dollars.

In March 2017, approximately five months before he resigned from ADI, Yu and his wife established Tricon, which, according to its website, “specializes in wide band MMIC amplifiers,” and serves customers in “defense and aerospace, test and instrumentation, [and] satellite communications.” On July 31, 2017, Yu allegedly resigned from ADI and signed an agreement affirming that he had surrendered all proprietary information or data.

Nevertheless, in December 2018 and again in June 2019, Yu allegedly had propriety ADI files in his possession both in his Google drive account and on his personal computers. Since creating Tricon in March 2017, Yu marketed and sold approximately 20 ADI designs as his own, and even used the same Taiwanese semiconductor fabrication plant as ADI to manufacture Tricon’s MMIC parts. The superseding indictment alleges that the defendants fraudulently obtained MMIC and other semiconductor parts from the Taiwanese semiconductor fabrication plant by providing the plant with ADI’s stolen designs and other proprietary information, and furthermore concealed the fact that the designs were stolen from ADI. (DMA, HSI, FBI, NCIS, CBP)

<https://www.justice.gov/usao-ma/pr/lexington-couple-and-their-semiconductor-company-indicted-charges-theft-trade-secrets>

ECONOMIC ESPIONAGE (18 U.S.C. § 1831)

- ***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 People’s Republic of China 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 (HSSD) conspirators sought to obfuscate the Chinese 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. The two-count indictment alleges that Ding Xiaoyang, Cheng Qingmin and Zhu Yunmin, were HSSD officers responsible for coordinating, facilitating, and managing computer hackers and linguists at Hainan Xiandun and other China Ministry of State Security (MSS) front companies to conduct hacking for the benefit of China and its state-owned and sponsored instrumentalities. The indictment alleges that Wu Shurong was a computer hacker who, as part of his job duties at Hainan Xiandun, created malware, hacked into computer systems operated by foreign governments, companies, and universities, and supervised other Hainan Xiandun hackers.

The conspiracy’s hacking campaign targeted victims across the world. Targeted industries included, among others, aviation, defense, education, government, health care, biopharmaceutical, and maritime. Stolen trade secrets and confidential business information included sensitive technologies used for submersibles and autonomous vehicles, specialty

chemical formulas, commercial aircraft servicing, and foreign information to support China's efforts to secure contracts for state-owned enterprises within the targeted country (e.g., large-scale high-speed railway development projects).

As alleged, the charged MSS Officers coordinated with staff and professors at various universities in Hainan and elsewhere in China to further the conspiracy's goals. Not only did such universities assist the MSS in identifying and recruiting hackers and linguists to penetrate and steal from the computer networks of targeted entities, including peers at many foreign universities, but personnel at one identified Hainan-based university also helped support and manage Hainan Xiandun as a front company, including through payroll, benefits, and a mailing address.

According to the indictment, to gain initial access to victim networks, the conspiracy sent fraudulent spearphishing emails that were buttressed by fictitious online profiles and contained links to doppelgänger domain names, which were created to mimic or resemble the domains of legitimate companies. In some instances, the conspiracy used hijacked credentials, and the access they provided, to launch spearphishing campaigns against other users within the same victim entity or at other targeted entities. The conspiracy also used multiple and evolving sets of sophisticated malware, including both publicly available and customized malware, to obtain, expand and maintain unauthorized access to victim computers and networks. The conspiracy's malware included those identified by security researchers as BADFLICK, aka GreenCrash; PHOTO, aka Derusbi; MURKYTOP, aka mt.exe; and HOMEFRY, aka dp.dll. Such malware allowed for initial and continued intrusions into victim systems, lateral movement within a system, and theft of credentials, including administrator passwords.

The conspiracy often used anonymizer services, such as The Onion Router (TOR), to access malware on victim networks and manage their hacking infrastructure, including servers, domains and email accounts. The conspiracy further attempted to obscure its hacking activities through other third-party services. For example, the conspiracy used GitHub to both store malware and stolen data, which was concealed using steganography. The conspiracy also used Dropbox Application Programming Interface (API) keys in commands to upload stolen data directly to conspiracy-controlled Dropbox accounts to make it appear to network defenders that such data exfiltration was an employee's legitimate use of the Dropbox service. (SDCA, NSD, FBI)
<https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion>

ALTERNATIVE CHARGES

- ***Saugus Woman Pleads Guilty to Trafficking Counterfeit Percocet Pills Containing Fentanyl.*** On September 30, 2021, Nicole Benton of Saugus, MA, pleaded guilty to conspiracy to manufacture, distribute, and possess with intent to distribute fentanyl and other controlled substances for her role in a large-scale drug trafficking organization that manufactured and distributed hundreds of thousands of counterfeit Percocet pills containing fentanyl. Benton was charged on June 30, 2021. According to the charging documents,

Benton was a member of a large drug trafficking organization (DTO) operated by Vincent Caruso, a self-admitted Crip gang member, that included Johnson and Vincent Caruso's mother, Laurie Caruso, among others. The DTO allegedly sold counterfeit prescription pills containing fentanyl – produced using multiple large pill presses capable of generating thousands of pills per hour– to street gangs for further distribution on the North Shore of Massachusetts. A single counterfeit fentanyl pill allegedly retails between \$10-\$20, thereby generating millions of dollars in retail sales. Benton admitted to distributing more than 100,000 pressed fentanyl pills on behalf of the organization. Based upon pills seized during the investigation, 100,000 pills would equate to more than 10 kilograms of fentanyl. During a search of Benton's residence on June 30, 2021, approximately 40 grams of fentanyl pills and a firearm were seized. (DMA, FBI, ATF, OCDETF)

<https://www.justice.gov/usao-ma/pr/saugus-woman-pleads-guilty-trafficking-counterfeit-percocet-pills-containing-fentanyl>

- ***Stamford Man Pleads Guilty to Trafficking Counterfeit Oxycodone Pills Containing Fentanyl Analogues.*** On August 6, 2021, Arber Isaku of Stamford, Connecticut, pleaded guilty to a charge related to his manufacturing and distributing counterfeit oxycodone pills containing fentanyl analogues. In April 2019, an indictment was unsealed charging Vincent Decaro, Arber Isaku, and David Reichard, all of Stamford, with offenses related to the trafficking of fentanyl analogues. The three-count indictment was returned on August 7, 2018. Decaro and Isaku, who were extradited from Albania, entered pleas of not guilty to the charges. As alleged in court documents and statements made in court, Decaro and Isaku purchased fentanyl analogues from suppliers in China and, working out of Decaro's residence at 77 West Hill Circle in Stamford, pressed the drug into counterfeit oxycodone pills, which they sold to customers on dark web markets. Reichard, who lived a short time at Decaro's residence, helped Decaro and Isaku press pills and mail the pills to customers. On April 3, 2018, a court-authorized search of Decaro's Stamford residence revealed numerous pills containing approximately 330 grams of fentanyl and acetyl fentanyl, approximately 40 grams of fentanyl analogues in powder form, three pill presses, instructions on how to prepare the fentanyl analogue Carfentanyl, a hazardous material suit, a gas/respirator-type mask, and numerous U.S. Postal mail envelopes. Prior to that date, on August 23, 2017, Isaku was arrested by the Connecticut State Police after he accepted delivery of a package containing approximately 160 grams of fentanyl at his residence in Stamford. At the time of the search of Decaro's home in April 2018, Decaro and Isaku were in Europe. They have been detained since September 21, 2018, when they were arrested by Albanian State Police as they were attempting to cross the border from Albania into Kosovo. A search of an apartment in Tirana where they had been staying revealed alprazolam, fentanyl and other controlled substances; tools and dies for pressing pills; and instructions for synthesizing fentanyl. Reichard was arrested on a federal criminal complaint on April 13, 2018. He previously entered a plea of not guilty to the charges in the indictment. (DCT, OIA, USPIS, DEA, CT State & Stamford Police, Albania State Police)

<https://www.justice.gov/usao-ct/pr/stamford-men-charged-trafficking-counterfeit-oxycodone-pills-containing-fentanyl>

<https://www.justice.gov/usao-ct/pr/stamford-man-pleads-guilty-trafficking-counterfeit-oxycodone-pills-containing-fentanyl>

- Ohio Man Sentenced for Distributing Counterfeit Pharmaceuticals in the Eastern District of Texas.*** On July 20, 2021, Austin Seymour of Uniontown, Ohio, was sentenced to federal prison for drug trafficking violations. Seymour pleaded guilty on January 26, 2021, to conspiracy to distribute and possess with intent to distribute controlled substances and was sentenced to 168 months. According to information presented in court, in February 2019, Seymour became the primary distributor for the Gary Collin Bussell drug trafficking organization and was responsible for the organization’s drug stash house. In so doing, he also assumed the role of the primary distributor to customers in the Dallas-Fort Worth area. He distributed counterfeit pharmaceutical pills, marijuana, and THC and was responsible for making payments to the organization’s narcotics suppliers. When a search was executed at Seymour’s residence, agents found a loaded Glock firearm in his vehicle along with various narcotics, bulk U.S. currency, a money counter, and a drug ledger in his apartment. Seymour was indicted by a federal grand jury on October 8, 2019, and charged with drug trafficking violations. (EDTX, DEA, OCDEF)

<https://www.justice.gov/usao-edtx/pr/ohio-man-sentenced-distributing-counterfeit-pharmaceuticals-eastern-district-texas>
- El Cajon Resident Pleads Guilty to Selling Counterfeit Pills that Caused Death of Nineteen-Year-Old.*** On July 8, 2021, Olatunde James Temitope Akintonde of El Cajon pleaded guilty, admitting that he sold fentanyl-laced pills that caused the death of a nineteen-year-old Santee man, identified in court records as S.J.G., in March of 2019. According to his plea agreement, Akintonde admitted that he sent messages to S.J.G. through social media on February 28, 2019, to coordinate the sale of what the victim believed to be oxycodone pills. Later that evening, Akintonde delivered two counterfeit oxycodone pills laced with fentanyl to S.J.G. After the meeting, Akintonde sent additional messages to S.J.G. through social media warning that he should only take one of the pills because they were “strong.” Akintonde further admitted in his plea agreement that the pills he gave to S.J.G. caused his death. According to other filings in the case, S.J.G. died in his home sometime in the evening of February 28, 2019 or the early morning hours of March 1, 2019. (DSCA, DEA)

<https://www.justice.gov/usao-sdca/pr/el-cajon-resident-pleads-guilty-selling-counterfeit-pills-caused-death-nineteen-year>
- Worcester Man Charged with Possessing Counterfeit Adderall Pills Containing Methamphetamine.*** On June 21, 2021, Nestiano Kristo of Worcester, MA, was charged by criminal complaint with possession with intent to distribute methamphetamine. According to the charging document, over the course of two months, Kristo allegedly sold significant quantities of counterfeit Adderall pills containing methamphetamine, cocaine, and suspected fentanyl to an undercover law enforcement officer. Specifically, on May 10, 2021, Kristo allegedly sold approximately 1,000 counterfeit Adderall pills containing 355 grams of methamphetamine and cocaine to the undercover officer. On June 21, 2021, agents recovered from Kristo’s residence over 50,000 suspected counterfeit Adderall pills, which are estimated to have a combined weight of over 17 kilograms; approximately one kilogram of suspected cocaine; and three firearms, one of which was modified into a fully automatic weapon. (DMA, DEA)

<https://www.justice.gov/usao-ma/pr/worcester-man-charged-possessing-counterfeit-adderall-pills-containing-methamphetamine>

- Reno Man Pleads Guilty to Selling Hundreds Of Counterfeit Oxycodone Pills Laced With Fentanyl.*** On May 26, 2021, Octavio Mendoza Jr. of Reno, CA, pleaded guilty to selling hundreds of counterfeit oxycodone pills containing fentanyl, a powerful synthetic opioid. According to court documents and admissions made in court, from June 12 to September 2, Mendoza sold counterfeit oxycodone pills stamped with “M30” that contained fentanyl. On September 6, law enforcement arrested Mendoza after observing him using drugs in a vehicle in downtown Reno. During a search of the vehicle, law enforcement found approximately 374 counterfeit oxycodone pills containing fentanyl. Mendoza pleaded guilty to seven counts of distribution of fentanyl and one count of possession with intent to distribute 40 grams or more of fentanyl. He was sentenced on December 7, 2021, to 34 months in prison followed by three years of supervised released. (DNV, FBI)
<https://www.justice.gov/usao-nv/pr/reno-man-pleads-guilty-selling-hundreds-counterfeit-oxycodone-pills-laced-fentanyl>
<https://www.justice.gov/usao-nv/pr/reno-man-sentenced-selling-hundreds-counterfeit-oxycodone-pills-laced-fentanyl>
- Florida Woman Sentenced to Six Months for Selling Counterfeit Medical Devices.*** On March 4, 2021, Janaina Nascimento of Hollywood, Florida, was sentenced to six months in federal prison, after previously being convicted of selling counterfeit Ethicon Surgicel® Original Hemostat (“Surgicel”), an absorbable surgical mesh used to control bleeding, that was ultimately purchased by the University of Kentucky Medical Center. Nascimento pled guilty to one count of introducing into interstate commerce a “misbranded” medical device, in violation of the Food, Drug, and Cosmetic Act. In her plea agreement, Nascimento admitted that in January 2019, she purchased 70 boxes of Surgicel from a distributor in the United Arab Emirates. When she attempted to re-sell the product to a United States purchaser, that buyer cautioned her that the Surgicel was not authorized for sale in the United States, pointing to a warning label on the box that stated “NOT FOR RE-EXPORT TO THE U.S.A.” Instead of investigating potential problems with the Surgicel, Nascimento removed individual packages of the product from their boxes with the warning label, and sold 828 such packages to a company called XS Supply, LLC, which then resold those 828 units to the University of Kentucky Medical Center, in April 2019. After complaints from several surgeons about the product, an investigation determined that the 828 units of Surgicel sold by Nascimento were a non-sterile counterfeit. Nascimento paid restitution of \$24,012 to the University of Kentucky Medical Center. (EDKY, FDA)
<https://www.justice.gov/usao-edky/pr/florida-woman-sentenced-six-months-selling-counterfeit-medical-devices>
- Pennsylvania Man Who Sold Counterfeit Prescription Pills Containing Fentanyl and Other Substances Pleads Guilty, Sentenced to More Than Four Years in Federal Prison.*** On December 3, 2020, Jacob Leister of Glenville, Pennsylvania, was sentenced to 51 months in federal prison, followed by three years of supervised release, after Leister pleaded guilty to distribution of fentanyl and Alprazolam. Leister was also ordered to forfeit \$15,400 in the form of a money judgment, which represents the net proceeds of his sale of drugs to an undercover officer. According to his guilty plea, from December 2018 through September 2019, Leister sold purported prescription pills to an undercover law enforcement officer on several occasions. As a result of these sales, Leister distributed at least 56 grams of a

mixture containing fentanyl and 708 pills containing Alprazolam. As detailed in his plea agreement, on three occasions between December 18, 2018, and February 7, 2019, Leister sold the undercover officer a total of 600 pills purported to be Alprazolam. In fact, the pills were found to contain flubromazolam, a substance similar to Alprazolam, which is not a controlled substance. The undercover officer paid Leister a total of \$15,400 for all of the pills. On November 21, 2019, Leister sold the undercover officer a large quantity of suspected Alprazolam pills, and he was then arrested by investigators. A search warrant was executed at Leister's residence that same day. Law enforcement recovered a number of computers, subsequent searches of which revealed information and photographs about bitcoin, cryptocurrency, and cryptocurrency exchanges, as well as information about dark web marketplaces where individuals can purchase drugs, among other things. (DMD, DEA, USPIS)

<http://www.justice.gov/usao-md/pr/pennsylvania-man-who-sold-counterfeit-prescription-pills-containing-fentanyl-and-other>

DEPARTMENT OF STATE

DEPARTMENT OF STATE

Department of State Appendix for FY 2021 Annual Report

This appendix discusses the Department of State's role in Intellectual Property Enforcement.

In FY 2021, the Department of State continued to promote international economic environments conducive to strong intellectual property (IP) regimes and thereby protect the products of U.S. ingenuity through efforts in Washington, DC, and in embassies and consulates around the world. The Department of State advocates for strong IP protection and enforcement in bilateral policy dialogues and in multilateral fora; collaborates with bilateral, interagency, and private sector partners on capacity building; monitors the state of IP protections and enforcement around the world to better address problem areas; and educates public and official audiences on the value of IP both to generate economic growth and to improve people's quality of life. Aligned with the Biden-Harris Administration's foreign policy for a middle class, better IP protection and enforcement abroad allows U.S. companies, including small to medium enterprises, to conduct business around the world with greater confidence.

The Department of State's lead on IP issues is the Office of Intellectual Property Enforcement (IPE), located in the Trade Policy and Negotiations Division in the Bureau of Economic and Business Affairs (EB) in Washington, DC. IPE participates in a range of interagency bilateral and multilateral efforts, conducts research and outreach, and serves a central support function on all IP matters for the agency's personnel. Areas in which U.S. embassies work with their host governments include increasing political will for strengthening copyright, patent, trademark, and other IP protections and their associated enforcement, as well as combatting forced technology transfer, online copyright piracy, and the production and sale of counterfeit goods. U.S. embassies and consulates report year-round on IP issues to keep Department of State headquarters and relevant U.S. government agencies up-to-date on key developments.

Department of State economic sections at embassies also liaise with local and global representatives of creative industries, manufacturers, and others about IP issues and advocate for U.S. rightsholders. State Department officials working on IP issues overseas collaborate with, and receive support from, many agencies, including the U.S. Patent and Trademark Office (USPTO) IP Attachés, Department of State-funded Department of Justice (DOJ) International Computer Hacking and Intellectual Property (ICHIP) advisors, and Department of Homeland Security (DHS) Homeland Security Investigation (HSI) representatives.

As the COVID-19 pandemic limited in-person work and travel throughout the fiscal year, the Department of State quickly shifted to maximum telework status. With in-person activities limited based on local pandemic conditions, the Department of State adopted widespread use of video-conferencing and other technologies. This enabled the Department of State to continue crucial bilateral dialogues, create and participate in a broad range of IP-related events and activities, discuss IP issues with interagency partners, and advance U.S. IP priorities overseas. What follows are illustrative examples of the broad, diverse range of work the Department of State performed on IP issues during the reporting period.

Diplomacy to Advance and Protect IP Rights

The United States has more than 270 diplomatic missions around the world. In addition to IPE efforts in Washington, DC, embassies and consulates feature Foreign Service Officers (FSOs) and locally employed staff who work to advance IP protection and combat IP infringement. They advocate for U.S. rightsholders and alert Department of State headquarters and relevant U.S. government agencies about opportunities to collaborate with the foreign governments and others, including to improve IP conditions by reviewing legislative and judicial matters, policy changes, and economic and political conditions that affect the IP environment. In addition to fulfilling Department of State activities on IP issues, the embassies and consulates support the overseas work of other U.S. government agencies through their economic sections, public affairs sections, and other Department of State offices. This assistance takes many forms including information gathering, diplomatic engagement to facilitate and coordinate bilateral discussions, participation in public IP-related events, organizing official U.S. government delegations addressing IP issues, and leading follow-up activities to high-level, IP-focused bilateral meetings.

Below are illustrative examples of the work that Department of State staff undertook during FY 2021.

Algeria: The U.S. Embassy in Algiers continued to support IP rights priorities. U.S.-Middle East Partnership Initiative (MEPI) funds supported the Department of Commerce's Commercial Law Development Program (CLDP) training in June 2021 with Algeria's technology transfer authority. MEPI also supported a CLDP review of franchising legislation, to include patent protections. The embassy earlier promoted CLDP's March 2021 virtual conference on empowering women entrepreneurs (which included a session on intellectual property as a business asset) through social media; there were 22 participants from Algeria. The embassy's public diplomacy section conducted a three-day training on *STEM from an American Perspective*, which included a session on IP and its importance to innovation.

Argentina: The U.S. Embassy in Buenos Aires coordinated with the regional ICHIP advisor to participate in a panel sponsored by the Argentine Anti-Piracy Association, a group of multinational firms self-organized to fight against IP infringement. The panel included Argentine judges and prosecutors, and the discussion focused on piracy and counterfeiting as a barrier to real economic development while supporting organized crime and terrorism.

Armenia: The U.S. Embassy in Yerevan collaborated with the Department of Commerce's CLDP to hold a virtual discussion on commercialization of research and technology transfer in Armenia with relevant Armenian government and business community representatives.

Azerbaijan: The U.S. Embassy in Baku advocated for IP protection through high-level engagement with host-country officials, public diplomacy engagement with the Azerbaijani public, and ongoing coordination with resident U.S. companies. As part of one continuing effort, Embassy Baku has been advocating for the end of unlicensed software use in the public and private sector in Azerbaijan, working closely with several U.S. software companies as part of this campaign. Through diplomatic engagement and foreign assistance, the embassy continues

efforts to promote IP enforcement in Azerbaijan to create a more transparent business environment for U.S. companies.

Bolivia: The U.S. Embassy in La Paz worked closely with Bolivia's National IP authority (SENAPI) and the Ministry of Productive Development and Plural Economy, to ensure that IP remains a regular bilateral topic of discussion. The embassy's direct outreach to the new Bolivian administration that assumed power in November 2020 resulted in productive dialogue on IP issues. The Bolivian government has expressed interest in strengthening bilateral cooperation and improving domestic IP protection and enforcement.

Cambodia: In October 2020, the U.S. Embassy in Phnom Penh coordinated the signing ceremony for a memorandum of understanding on the accelerated approval of patent applications, between the head of the USPTO and the Cambodian minister of Industry, Science, Technology, and Innovation. The MOU expedites the process to recognize U.S. patents in Cambodia, protecting U.S. patent holders and strengthening Cambodia's investment climate.

Canada: In March 2021, U.S. Embassy Ottawa, in partnership with the Internet Society of Canada, hosted a research integrity event for Canadian academic and government officials that focused on threats from foreign actors to academic research and viable mitigation strategies to protect research, including valuable IP. The panelists detailed vulnerabilities to the U.S. research system from foreign threats, particularly those related to the People's Republic of China's (PRC's) military-civil fusion ambitions. They also focused on weaknesses in how the U.S. research community approaches foreign engagement risk and recommended that Canadian research institutions take a proactive risk assessment and management process that catalogs assets, identifies threats, analyzes gaps, ranks risks, and creates counter measures.

Denmark: The U.S. Embassy in Copenhagen regularly incorporated messaging on the importance of IP protection in its social media content. For example, the embassy posted IP fact sheets; joint statements highlighting the U.S.-EU partnership on security telecommunications infrastructure; the IP discussion that took place as part of the Secretary of State's visit to Denmark in May 2021; and promotion materials on the occasion of World IP Day in April 2021.

Egypt: In September 2021, officials from the Egyptian Ministry of Higher Education, the Academy of Scientific Research and Technology (ASRT), the Science and Technology Development Fund, and technology transfer offices at public and private universities participated in a three week International Visitor Leadership Program (IVLP) on unlocking the value of intellectual property through the commercialization of research.

Jamaica: In May 2021, the U.S. Embassy in Kingston launched the U.S. and Jamaican EdTech Women Providing Opportunities for Women's Economic Rise (POWER) Connect initiative, which is funded through the Department of State Bureau of Economic Affairs' POWER program to support women's entrepreneurship and economic empowerment. One of the sessions focused on marketing, branding, and licensing educational technology (EdTech) products, including how female EdTech entrepreneurs can protect their IP.

Pakistan: The U.S. Embassy in Islamabad, in collaboration with and supported by the Department of Commerce's CLDP, conducted six virtual engagements (January to May 2021) as part of a program focused on *Countering Counterfeit Pharmaceuticals and Medical Devices*. The online engagements brought together officials from Pakistan's Federal Bureau of Revenue (FBR), Customs, and the Intellectual Property Office (IPO), as well as representatives of Pakistani, U.S., and other international pharmaceutical companies operating in Pakistan. Officials from USPTO, the Food and Drug Administration, and Customs and Border Protection (CBP) joined CLDP attorneys and subject matter experts. The engagements facilitated an exchange of best practices between the involved agencies of both countries with the intent of holding a future, in-person, joint exercise focused on counterfeit interdiction at a Pakistani port of entry. IP enforcement is the weakest link in Pakistan's IP regime. Pakistani officials cited this program as a key mechanism to improve Pakistan's capacity to identify counterfeit products and safely interdict illicit trade via Pakistani ports.

Papua New Guinea: The U.S. Embassy in Port Moresby arranged for an employee in Papua New Guinea's Investment Promotion Authority and another employee from the Solomon Islands Registrar General's Office to participate in a Department of State Bureau of Educational and Cultural Affairs' virtual International Visitors' Leadership Program on *Intellectual Property Rights Regulation Formation* held over three weeks in April and May 2021. Participants in this program examined policies, strategies, and mechanisms supporting and protecting IP across a variety of sectors, and they explored methods for implementing and enforcing legal codes and policies to combat IP theft. The program also focused on the value of intellectual property created by state-funded research and the benefits that can accrue to all stakeholders. Participants met with U.S. officials, private sector stakeholders, and industry groups to understand how the United States identifies and counteracts IP infringement and customs fraud through direct exposure to the U.S. IP system.

Rwanda: The U.S. Embassy in Kigali conducted a webinar with a Loyola College of Law professor to share insights on IP legal issues. The event established an on-going exchange of views with members of the Rwanda Ministry of Trade and Industry as well as the Rwanda Development Board.

Seychelles: The Port Louis-based U.S. Embassy in Mauritius and Seychelles organized training on copyrights, designs, and trademarks for students of the Seychelles Institute of Art and Design in July 2021.

Slovenia: In July 2020, Embassy Ljubljana provided a \$9,000 grant to the Slovenian NGO Intellectual Property Institute (IPI) to implement a project called *Intellectual Property and Artificial Intelligence: Legal Challenges for Text and Data Mining and Big Data Analytics*. The project allowed IPI to share knowledge on copyrights related to artificial intelligence and machine learning with Slovenian researchers and businesses, enabling them to avoid potential copyright infringements in their research and commercial activities. Between October 2020 and April 2021, the project resulted in six virtual events that reached more than 1,000 participants, new online resources including a dedicated IPI webpage that highlight protections of IP for research and commercial activities, and greater cooperation between IPI and American

University's Washington College of Law Program on Information Justice and Intellectual Property.

South Africa: The U.S. Mission in South Africa worked closely with South African businesses, law enforcement, and customs authorities during FY 2021 to increase IP enforcement capacity and strengthen public-private IP investigation cooperation to counter increasingly sophisticated methods of IP theft. Representatives from the Mission's HSI unit and economic section joined local law firms and law enforcement on two market surveillance exercises to gain greater understanding of the complexities of civil and criminal IP investigations on the ground to better target IP-focused assistance.

Tajikistan: The U.S. Embassy in Dushanbe shared information on IP and the financial harm caused by copyright piracy through the embassy's social media accounts. Those social media posts reached 5,370 people. In addition, two separate social media posts featuring IP-focused quizzes reached more than 4,000 users, helping to better educate the Tajik population about the importance of IP protection.

Uruguay: An economic officer at the U.S. Embassy in Montevideo provided opening remarks on IP issues at two separate seminars about trademark enforcement. In addition, the embassy's economic and commercial officers organized discussions with U.S. firms regarding Uruguay's patent protections which lead to discussions with Uruguay's Ministry of Foreign Affairs on provisional patent protection.

Washington, DC: In October 2020, IPE staff served on the multi-agency panel of a USPTO webinar on *How the U.S. Government Can Help Companies Protect and Enforce their IP in China*. The event provided viewers with information on U.S. government services available to U.S. firms facing IP challenges in Asia.

Washington, DC: In December 2020, IPE staff virtually participated in the Business of IP Asia Forum, an annual gathering for IP experts and business leaders to exchange views on cutting-edge IP issues. This year's event focused on the jurisdictional challenges of IP protection and enforcement in the developing Greater Bay Area comprised of Hong Kong, Macao, and the PRC.

World Intellectual Property Day

The Department of State strives to raise IP awareness internationally through ongoing public diplomacy events and celebrates World Intellectual Property Day ("World IP Day") on April 26 as the flagship annual engagement.

For the 2021 World IP Day, the World Intellectual Property Organization (WIPO) suggested a theme focused on small- and medium-size enterprises (SMEs): *IP and SMEs: Taking Your Ideas to Market*.

On April 23, 2021, President Biden issued a proclamation recognizing April 26, 2021, as World IP Day to "celebrate the innovators and creators who enrich our lives and create the products, services, companies, and industries of tomorrow" (<https://www.whitehouse.gov/briefing->

[room/presidential-actions/2021/04/23/a-proclamation-on-world-intellectual-property-day-2021/](https://www.state.gov/presidential-actions/2021/04/23/a-proclamation-on-world-intellectual-property-day-2021/)). In the proclamation, the President highlighted the importance of IP to small businesses and their ability to grow, compete, and support their communities. In support of this proclamation and the WIPO theme, the Department of State posted on its website and on social media a video featuring how these businesses can use IP for post-pandemic recovery and increase their competitiveness and resiliency. The video was the State Department Bureau of Economic and Business Affairs' top media tweet for April 2021 (<https://www.state.gov/world-intellectual-property-day/>).

The Department of State marked World IP Day by engaging in a wide range of activities around the world, which included the following.

Armenia: In celebration of World IP Day on April 26, the U.S. Embassy in Yerevan conducted a social media campaign highlighting Armenian leaders in the IP space and their efforts related to voluntary technology transfer.

Azerbaijan: The U.S. Embassy in Baku hosted an online discussion with local entrepreneurs on the theme of “building a business out of intellectual property” to mark World IP Day. Delivering opening remarks for this event, the U.S. ambassador emphasized the important role IP protection plays in fostering innovative economies in the U.S. and around the world. Local panelists shared their experiences building businesses out of an idea and emphasized the importance of protecting IP to promote business growth. Within just one day of the event, the program recorded more than 1,100 views, 51 likes, and 26 comments.

Bolivia: The U.S. Embassy in La Paz participated in a regional workshop on IP issues on April 22 funded by the Bureau of Educational and Cultural Affairs' Arts Envoy Program. During the event, a U.S. singer-songwriter demonstrated how IP protections help aspiring artists. Approximately 80 percent of the 200 online participants were from Bolivia.

Botswana: The U.S. Embassy in Gaborone – in collaboration with State EB, State IPE, and Botswana's Companies and Intellectual Property Authority – produced a World IP Day program with U.S. and Botswana speakers, who shared their personal experiences and practical advice with local entrepreneurs related to the WIPO theme. During the event, a senior advisor in State EB interviewed a U.S. inventor who explained how IP helped her start her business and how she relies on IP protection on a daily basis.

Cambodia: To mark World IP Day 2021, the U.S. ambassador to Cambodia hosted a virtual discussion on the important role IP protection plays in creating economic growth and supporting artistic innovation. The panel featured three Cambodian recording artists and entrepreneurs and a local distributor of Hollywood films. The event was pre-recorded and posted on the Embassy's Facebook page. It received 12,600 views and 1,300 likes from the public.

Canada: Forty-two U.S. and Canadian SMEs joined U.S. Mission Canada's April 26 World IP Day event – *Small Business; Big Ideas: Protecting Your IP*. The objective of the webinar was to engage SMEs on the importance of IP tools and resources they can use to protect and enforce IP. The then-chargé d'affaires gave opening remarks on the importance of IP to the U.S. administration's commitment to help SMEs recover from COVID-19, noting women-owned,

indigenous-owned, and minority-owned businesses have been disproportionately affected by the pandemic. The Canadian Intellectual Property Office (CIPO) interim CEO closed the event by echoing the importance of supporting SMEs in their efforts to acquire and use IP to grow their businesses. The event featured expert speakers from the USPTO Global IP Academy, the Canadian Intellectual Property Office (CIPO), the U.S. Department of Commerce's International Trade Administration STOPFakes program, and the Canada Border Services Agency.

China: The U.S. Embassy in Beijing celebrated World IP Day through a collaboration with the embassy's public affairs section, the Beijing Patent and Trademark Office, and the Cornell-Tsinghua Executive MBA Program during a May 9 panel discussion for students. The in-person event before an audience of approximately 60 attendees was also broadcast online. The embassy's USPTO IP Counselor moderated the panel of entrepreneurs, lawyers, and investors, with the focus on the value in creating and developing IP (versus acquisition), IP protection, and the importance of SMEs to the global economy.

Chile: The U.S. Embassy in Santiago promoted bilateral cooperation in IP rights protection through a virtual World IP Day event on May 4 on *Protecting Intellectual Property of SMEs Entering Foreign Markets*. The embassy and the Technical Cooperation Service (SERCOTEC), which is Chile's lead agency for the promotion of SME development, co-organized the event, which gave SMEs the opportunity to learn about the U.S. patent and trademark application processes from USPTO attorney advisors based in Washington, DC and in Lima. The event also included a presentation by the director of the National Institute of Industrial Property, Chile's lead IP protection agency, about how Chilean SMEs can benefit from the advantages of Chile's accession to the Madrid Protocol. The event attracted almost 300 participants, mostly SME entrepreneurs and SERCOTEC advisors, who work at Chile's network of small business development centers. SERCOTEC surveys following the event showed that over 90 percent of participants rated the event positively, and 80 percent expect to apply the information they gained to their businesses. The embassy's economic section is using information from the event to design a future training module, focused on SME patent and trademark issues, that incorporates feedback from both U.S. and Chilean IP agencies.

Costa Rica: The U.S. Embassy in San Jose celebrated World IP Day with music. The embassy, in partnership with Costa Rica's Ministry of Foreign Trade and National Intellectual Property Rights Registry, organized an April 27 program that celebrated Costa Rica's recent removal from the U.S. Trade Representative Special 301 Report and underscored the importance of registering one's IP and respecting the IP of others. The event focused on key universities and innovation hubs with support from the Department of State's Bureau of Educational and Cultural Affairs (ECA) entrepreneurship programs, including the Academy for Women Entrepreneurs and the Young Leaders of the Americas Initiative. The program explored the importance of IP and featured stories of successes that Costa Rican businesses have had related to trademarks. The program included a mix of pre-recorded videos and live remarks (from the embassy's charge d'affaires and Costa Rican government officials), as well as songs and remarks by a U.S. acapella group that visited Costa Rica through a Department of State ECA-supported Arts Envoy program.

Ecuador: U.S. Embassy Quito's World IP Day virtual event highlighted the importance of IP protection to safeguard firms' brands and ideas. Participants from the Ecuadorian Ministry of Production, Trade, Investment and Fisheries, the National Service of Intellectual Service of Intellectual Property Rights, and three private sector companies joined the U.S. ambassador to raise awareness of the importance of IP for business growth in a country aiming to support SMEs during a pandemic-induced recession. The Embassy also produced a video featuring the U.S. ambassador for both the World IP Day virtual event and for Embassy social media highlighting how IP helps small businesses protect their ideas and business models.

France: The U.S. Embassy in Paris published social media messages in French to promote World IP Day on April 26 to encourage SMEs to innovate. On the embassy's Twitter and Facebook accounts, the IP social media messages reached 3.5K people and attracted 44 positive user engagements, including a retweet from the French Association Against Counterfeiting (Association française de lutte anti-contrefaçon).

Haiti: The U.S. Embassy in Haiti released a social media message in English, French, and Creole in observance of World IP Day.

Jamaica: The U.S. Embassy in Kingston participated in the Jamaican Intellectual Property Office's (JIPO) Intellectual Property week from April 23-29, which focused on how small- and medium-size enterprises can take their ideas to market. An embassy official participated in a panel discussion on World IP Day that focused on IP enforcement and discussed ways that the U.S. Embassy in Jamaica worked with JIPO and the Jamaica Constabulary Force to protect IP and seize counterfeit goods.

Japan: The U.S. Embassy in Tokyo held a roundtable focused on the WIPO theme of *IP and SMEs: Taking our ideas to market*, with a specific focus on healthcare. The discussion focused on the difficulties SMEs face in navigating and leveraging the global IP system, and technology trends that make IP even more important for SMEs (particularly those related to the healthcare sector) to find their niche, brand themselves, and compete. The virtual program featured a keynote speaker followed by a panel discussion with IP and SME experts. Nearly 150 representatives of the Japanese government, business associations, and SMEs attended the event.

Kosovo: The U.S. Embassy in Pristina's economic section, public diplomacy section, and the U.S. Agency for International Development (USAID) collaboratively designed multiple World IP Day 2021 engagements. The embassy used the accomplishments of Kosovo musicians, filmmakers, and artists to educate key audiences about the costs of IP theft. The social media campaign (#ProtectCreativeKosovo) was shared and amplified by famous local artists, film directors, the Cinematographic Institute, a prominent film studio, and the Kosovo Consulate in Iowa, bringing widespread attention and increasing awareness about IP protection. One Facebook post attracted more than 6,000 engagements and reached over 63,500 users. At the invitation of the American Chamber of Commerce in Kosovo, FSOs participated in a World IP Day panel alongside legal experts and leaders of the Kosovo Intellectual Property Agency and Kosovo Customs. The discussion was wide-ranging and included alternative dispute resolution mechanisms, considerations for entering foreign markets, and local institutional barriers to IP protection. The event reached 2,780 Facebook users and garnered 516 engagements. USAID Kosovo's Commercial Justice Activity (the Activity) teamed with the Innovation Center Kosovo

(ICK) to mark World IP Day on April 26 by delivering a livestreamed roundtable. Targeting innovative business startups to build knowledge and raise awareness, this event gathered IP experts and private sector representatives to explain how IP protections help new businesses thrive and innovate. The event attracted 3,100 views. The Activity later supported a two-day IP training program through the Kosovo Justice Academy on May 11-12, and 17 judges participated in the pilot delivery. On May 27, the Activity delivered an IP mentoring session at ICK's Startup Bootcamp to more than 30 aspiring *Techstars* businesses.

Kuwait: In recognition of World IP Day 2021, U.S. Embassy Kuwait engaged with a popular, local graphic artist to develop a comic strip highlighting the importance of copyright protection for emerging artists. The embassy posted the comic strip on its social media sites on World IP Day where it attracted broad, positive attention. The embassy coordinated with the artist, the recently-established Kuwait Copyright Office, and the American Chamber of Commerce to repost the graphic, thereby increasing audience reach. Additionally, the U.S. Ambassador noted U.S.-Kuwait IP cooperation through a tweet that tagged the various Kuwaiti government agencies with IP responsibilities.

Mexico: The U.S. Embassy in Mexico City marked World IP Day by sharing via social media President Biden's World IP Day proclamation and other information about IP's importance.

Moldova: To raise awareness of IP issues and provide best practice solutions, the U.S. Embassy in Chisinau partnered with local business associations and IP special agents with the HSI unit to host a roundtable on World IP Day 2021. The discussion helped business association members learn about the IP resources available through the DHS ICE/HSI IPR Center, as well as best practices for businesses to identify and safeguard their operations and products against IP infringement.

Netherlands: The U.S. Embassy in The Hague held a bilateral meeting with representatives from the Dutch government to mark World IP Day. The focus of discussions centered on the strong bilateral relationship between the two partners and ways to work together on IP issues related to combatting climate change, COVID-19, and IP theft.

Peru: The U.S. Embassy in Lima led a regional virtual concert series that brought together more than 705 participants from Peru, Bolivia, Colombia, and Venezuela to highlight the importance of protecting IP rights. The initiative included a series of virtual events with a U.S. singer-songwriter who illustrated through original songs the importance of copyright protection for creative performers, producers, and innovators. Funded by the Bureau of Educational and Cultural Affairs' Arts Envoy Program, the concerts reached stakeholders and future leaders on IP issues, including entrepreneurs, young artists, and university students.

Philippines: The U.S. Embassy in Manila used two World IP Day events in April to address an information gap related to IP enforcement and technological innovation. In partnership with the Philippine government's Optical Media Board and the U.S. DOJ's ICHIP program, the U.S. Embassy in Manila virtually convened a workshop for 150 IP rights enforcers from the 10-member National Committee on Intellectual Property Rights of the Philippines (NCIPR), Department of Information and Communications Technology, and the Office of the Special Envoy on Transnational Crime. The workshop shared best practices on the online investigation

of IP crimes. Participants gained expertise in identifying online criminals, investigating online criminals, and preserving evidence from third-party providers. Separately, the embassy organized a live panel discussion on *IP and Environment: Innovations in Green Technology* to celebrate World IP Day and in honor of Earth Day. The panel, which brought together more than 300 entrepreneurs, academics and inventors, featured IP experts and social entrepreneurs, who highlighted the role of IP assets in supporting the development of green technological innovations. The social entrepreneurs shared how they incorporated green and sustainable initiatives in their enterprises and discussed how IP protection enhanced their value propositions, helped foster environmental innovation, and supported products that can help meet U.S. and Philippine climate targets. IP practitioners complemented the discussion with a presentation on integrating IP into an enterprise's business model. The audience engaged actively with the panel during the question-and-answer session.

Poland: The U.S. Embassy in Warsaw organized a virtual event on April 26 on *Local to Global: The Role of IP Management in Technology Transfer* to celebrate World IP Day. The chargé d'affaires opened the event, followed by a discussion panel of three IP experts from the United States and Poland. Forty people participated in the online event, largely consisting of entrepreneurs, start-ups and SME owners, representatives of the university transfer technology centers, and science and technology centers. The event emphasized the importance of modern IP systems for building stronger and more resilient businesses to be ready for international expansion.

Saudi Arabia: The U.S. Mission Saudi Arabia used social media to promote World IP Day.

Seychelles: The Port Louis-based U.S. Embassy in Mauritius and Seychelles held two events to celebrate World IP Day in Seychelles. The first event was a two-day workshop targeted at SMEs which started with a basic course led by State IPE. On the second day, a musician who is a strong advocate for IP protection explained the importance of copyright to her livelihood and advocated for strong IP protection related to streaming music platforms and international laws on copyright protection.

Tunisia: The U.S. Embassy in Tunis' public affairs section partnered with USPTO's regional IP Attaché and a Tunisian firm licensing U.S. technology on an April 26 webinar to celebrate World IP Day. The event drew over 30 participants.

Vietnam: To celebrate World IP Day, the U.S. Consulate General in Ho Chi Minh City, USAID's Linkages for Small and Medium Enterprises (LinkSME) project, and the U.S.-ASEAN Connect Digital Economy Series jointly organized an April 26 hybrid forum. The event brought together representatives of approximately 200 Vietnamese SMEs in-person and virtual participants from around Southeast Asia for a broad range of discussions on how protecting brands, data, and IP is critical for SMEs as they adopt digital transformation strategies. Government and private sector officials underscored the growing challenge of IP enforcement in the digital realm, while representatives from online platforms and services showcased tools to enable SMEs to access the digital economy.

Washington, DC: State IPE organized a webinar for a global audience that featured a panel of U.S. entrepreneurs who shared their IP journeys, including a discussion of the issue of counterfeits.

Multilateral Engagement

The Department of State works closely with our interagency partners to ensure U.S. views are known and incorporated in global regulatory, standard-setting bodies and in trade-focused organizations. The Department of State participates in U.S. delegations to multilateral forums and international organizations with global IP protection and enforcement implications including the World Trade Organization's (WTO's) Council for Trade-Related Aspects of Intellectual Property Rights (TRIPS Council), the World Health Organization (WHO), the Organization for Economic Co-operation and Development (OECD) Task Force on Countering Illicit Trade, the World Intellectual Property Organization (WIPO), the World Customs Organization (WCO) Enforcement Committee, the Intellectual Property Rights Experts Group (IPEG) of the Asia-Pacific Economic Cooperation (APEC) Forum, the Group of 7 (G7), the Group of 20 (G20), and various United Nations (UN) bodies.

Within such multilateral fora, State IPE participates in interagency processes to review resolutions, declarations, and other statements and ensure that U.S. IP priorities are accurately reflected. Depending on the venue and in the event that multiple rounds of negotiations do not result in a document that reflect U.S. views, an Explanation of Position or an Explanation of Vote may be issued to clarify U.S. policies. A few examples of multilateral documents containing IP equities issued in 2021 include the World Health Assembly's *Strengthening local production of medicines and other health technologies to improve access*, the World Health Assembly's *Strengthening WHO preparedness for and response to health emergencies*, multiple resolutions for the UN's Human Rights Council, the UN's Ministerial Declaration for the High-Level Political Forum on Sustainable Development, the *G7 Carbis Bay Communique*, and the *G20 Rome Declaration*.

The United States reports on its incentives to promote and encourage technology transfer to least-developed country (LDC) WTO members in the annual Article 66.2 Report. IPE receives input from missions overseas, regional and functional bureaus, and interagency partners on the range of U.S. government technology transfer and capacity building activities around the world. IPE submits the Article 66.2 Report to the WTO TRIPS Council annually. The broad range of activities covered in this report – including laboratory-based scientific collaboration, capacity building and education, and IP enforcement activities – highlight the United States' efforts to promote effective and voluntary transfer of technology to LDC members.

The United States also engaged at the WTO TRIPS Council in FY 2021 on proposals related to the COVID-19 pandemic response. Extraordinary circumstances call for extraordinary measures, so in May 2021, in service of ending the pandemic, the United States announced support for a waiver of IP protections for COVID-19 vaccines under the WTO TRIPS Agreement. IPE oversaw the Department of State's response to inquiries on this policy, including by supporting and coordinating with U.S. embassies and consulates around the world.

Other activities that the Department of State participated in during FY 2021 include the following.

- In October 2020, IPE leadership attended the first Global Intellectual Property Challenges Forum. While not an official G20 event, the virtual gathering brought together representatives of G20 members' IP agencies to discuss responses to the COVID-19 pandemic.
- IPE leads the U.S. delegation to the OECD Task Force on Countering Illicit Trade (TF-CIT). The Department of State's Deputy Assistant Secretary for Trade Policy and Negotiations gave one of the two keynote speeches at the TF-CIT's ninth annual meeting, which was held in March 2021. The remarks linked U.S. efforts to fight illicit trade, including IP infringement, with the new U.S. Administration's trade and national security principles.

Investment Climate Statements

Every year, economic officers at U.S. embassies and other diplomatic missions prepare Investment Climate Statements analyzing more than 170 foreign markets to help U.S. companies make informed business decisions regarding overseas investments and operations. Each Investment Climate Statement focuses on an individual country market and includes a chapter on IP. These Statements also form a chapter of the Department of Commerce's Country Commercial Guides and can be read together with those guides for a broad description of the investment and business environments in foreign economies. The State Department continues to work with the Department of Commerce to further align the complementary Statements and Guides for a more unified experience for the end user.

Science and Technology Agreements (STAs)

The United States finalized STAs with Greece, Georgia, Estonia, Israel and Serbia. All included IP annexes.

Interagency Policy Cooperation

IPE, working with U.S. embassies and consulates around the world, engages with U.S. stakeholders and foreign governments to ensure that the U.S. government's positions are informed by the full range of views on pertinent issues, and encourages trading partners to engage fully and transparently with the full range of IP stakeholders. These thorough "on-the-ground" explorations of overseas IP environments support bilateral policy decisions by deepening U.S. departments' and agencies' knowledge. For example, the Department of State provided extensive support to the Office of the U.S. Trade Representative (USTR) and interagency colleagues for USTR's IP-related reports, including the annual Special 301 Report and Review of Notorious Markets for Counterfeiting and Piracy. At IPE's request, posts around the world submitted detailed analyses of IP protection and enforcement conditions, as well as insights into trademark counterfeiting and copyright piracy.

The International Visitor Leadership Program

The International Visitor Leadership Program (IVLP) is the U.S. Department of State's premier professional exchange program. Through short-term projects (held in the United States when circumstances permit), current and emerging foreign leaders in a variety of fields experience the United States firsthand and cultivate lasting relationships with their American counterparts. Professional meetings reflect the participants' professional interests and support the foreign policy goals of the United States.

In fiscal year 2021, ECA organized three virtual IVLP projects related to IP:

- *Intellectual Property Rights Formation*, a project geared toward the East Asia and Pacific region. Participants in the April/May 2021 project were from Papua New Guinea, New Zealand, and Fiji.
- *IPR Enforcement and Protection in the United States*, a July 2021 project for participants from the People's Republic of China.
- *Technology Transfer and Intellectual Property Commercialization*, a project for participants from Egypt held in September 2021.

The U.S. Transnational and High-Tech Crime Global Law Enforcement Network International Computer Hacking and Intellectual Property (ICHIP) Advisor Program

The U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN) consists of Global Cyber Forensic Advisors (GCFAs) and International Computer Hacking and Intellectual Property (ICHIPs) Advisors, who are experienced DOJ prosecutors posted at U.S. overseas missions to strengthen regional enforcement coordination and deliver capacity building training. ICHIPs are located in Panama City, Panama; Zagreb, Croatia; Addis Ababa, Ethiopia; The Hague, Netherlands; Hong Kong, China SAR; Sao Paulo, Brazil; Bucharest, Romania; Abuja, Nigeria; Bangkok, Thailand; and Kuala Lumpur, Malaysia. In addition, two ICHIPs are deployed out of Washington, DC, to specifically address dark market/cryptocurrency and online consumer protection-related aspects of cybercrime and IP theft.

The GLEN is almost entirely funded and managed by the Department of State INL/GPP with the exception being ICHIP Bangkok, who is funded by the Department of Justice and staffed by DOJ personnel. The GLEN works with foreign countries to strengthen IP protection and enforcement leading to more effective investigation and prosecution of IP offenses. INL/GPP consults closely with IPE in program development and implementation.

The ICHIPs have regional responsibilities to: (1) assess the capacity of law enforcement authorities throughout the region to enforce IP; (2) develop and deliver training and other capacity building formats designed to enhance the capacity of justice sector personnel to enforce IP; (3) assist in developing or strengthening institutions dedicated to enforcing IP; (4) monitor regional trends in IP protection and computer crimes; and (5) provide expert assistance in support of U.S. IP and computer crimes policies and initiatives in the region. The GCFAs, in

coordination with ICHIPs, deliver digital forensics training for investigators, while the long-term federal agent mentors are designed to be paired with an ICHIP to deliver sustained mentoring to foreign counterparts.

INL also provides funding to the DHS ICE/HSI IPR Center and the USPTO to deliver foreign law enforcement training and technical assistance to complement the work of the GLEN. DHS and USPTO-delivered workshops ensure that patent and trademark agencies and foreign border and customs agencies receive IP enforcement capacity building tailored to their missions. DHS and USPTO programming is closely coordinated with the work of the GLEN. INL funds also support DHS providing U.S. trainers to participate in INTERPOL-managed IP workshops around the world.

Capacity Building and Training

The Department of State, using foreign assistance anti-crime funds managed by INL, has a longstanding program to provide U.S. government capacity-building training and technical assistance to foreign law enforcement partners to combat IP crime and to deter widespread commercial-scale pirated and counterfeit goods and services. The Department of State works with other agencies to prioritize assistance to developing countries that are named in USTR's Special 301 Report as countries of concern.

Examples of training successes through the ICHIP program include the following.

- ICHIP São Paulo mentored officials of Brazil's Ministry of Justice and Public Security, who seized approximately 330 websites and mobile applications that facilitated the illicit streaming and/or downloading primarily of films, television series, and live sporting events. This was part of the second phase of Operação 404 (Operation 404), a website and domain-blocking operation that targets online digital pirates who stream copyrighted content (dismantling over 200 websites, including several registered in the U.S., and arresting website administrators throughout Brazil). This was the largest-ever takedown of its type in Brazil. Authorities also removed advertisements of these services from social media platforms and de-indexed them from leading search engines to limit their availability to users. Pursuant to judicial order, visitors attempting to access the seized sites were redirected to a Brazilian government server hosting a banner declaring the site has been removed for violations of law. Civil Police also executed eighteen search warrants at multiple locations in multiple states including Sao Paulo, Minas Gerais, Rio Grande do Norte, and Santa Catarina, while authorities also detained the administrators of sites seized by the U.S. Attorney for the Eastern District of Virginia with ICHIP support. The São Paulo ICHIP provided numerous trainings throughout Brazil and Latin America and the Caribbean on counterfeit pharmaceuticals and fraud connected to COVID-19 vaccines, and in celebration of World IP Day hosted an online event with the private sector to demonstrate techniques and best practices to combat third-party vendor counterfeiting on online platforms. The São Paulo ICHIP also mentored police and prosecutors in São Paulo and Rio, who have seized and are prosecuting large-scale manufacturers and sellers of counterfeit goods; this includes an online counterfeit shoe

vendor found in possession of over \$20 million USD in counterfeit shoes, and a perfume counterfeiter responsible for fabricating over \$100 million USD in counterfeit fragrances.

- ICHIP Hong Kong worked with Vietnamese prosecutors and the judiciary to help Vietnam enact significant revisions to its criminal IP statute. The Vietnam Supreme People’s Court requested and received assistance for the lower courts on the proper implementation of the new laws. The ICHIP facilitated U.S. experts to assist with the drafting process for a judicial resolution on the new laws and organized a judicial workshop.
- ICHIP Abuja created roundtable working groups consisting of select alumni from its several regional pharmaceutical crime and IP enforcement workshops for continuing engagement and formal follow-up/case mentoring, with the support of private sector rightsholders. Many are also serving as ambassadors for the work the group is doing, spearheading national groups in Sierra Leone, the Gambia, and Namibia.
- The Washington, DC-based ICHIP for Internet-Based Fraud and Public Health participated in delivery of a webinar series on online investigations of counterfeit pharmaceuticals for Bulgarian law enforcement, moderating a discussion with three COVID-19 vaccine manufacturers who shared examples of the latest fraud and counterfeits that target the public, governments, and the medical supply chain.
- ICHIP Panama worked with Jamaican officials to address capacity-building needs for law enforcement officials in the wake of the cyberattack on the Jamaican Government COVID-19 website, including how to obtain electronic evidence from U.S. providers, emerging trends and challenges in digital forensics, best practices for seizing cryptocurrencies, and extracting data from encrypted or passcode-protected devices. The ICHIP agreed to serve as a bridge to the appropriate liaisons in key Jamaican ministries and agencies.

In addition, in FY 2021, IPE assumed a coordinating role to generate meaningful results of the IP training programs that multiple federal agencies conduct overseas. Working with interagency partners, IPE compiled a list of the IP-related trainings, identified priority countries where the United States may be able to make real progress, and started the process of developing coordinated training plans to maximize both U.S. resources and impact.

Internal Education Activities

The Department of State is committed to educating its employees about IP issues. IPE, in partnership with USPTO’s Global IP Academy, coordinated a two-day virtual training course on IP issues for U.S. government officials in July 2021. The course, which is usually held in-person at the USPTO, was held virtually because of the COVID-19 pandemic. Most participants were FSOs preparing for onward assignments domestically or overseas. The training also included civil servants and locally employed staff of U.S. overseas diplomatic posts. Experts and stakeholders briefed attendees on IP fundamentals, U.S. government positions on current IP “hot topics,” and U.S. industry priorities. These officials are now better equipped to advocate for

U.S. rightsholders and to articulate U.S. government policy positions in bilateral discussions and in international fora.

IPE also trained FSOs, locally employed staff, and representatives from various U.S. government agencies in sessions of the Foreign Service Institute's classes on Commercial Tradecraft. The training provided participants with the latest U.S. policy perspectives on international IP issues, enabling them to advocate better for U.S. rightsholders overseas.

In addition, in FY 2021, IPE launched a specialized, ongoing webinar series to brief Department of State employees in Washington and around the world on timely issues. Topics have included preparing IPE information for interagency use, regional discussions on the DOJ's ICHIP program, and an interagency panel discussion on current global IP protection and enforcement challenges, including counterfeits.

DEPARTMENT OF TREASURY

DEPARTMENT OF TREASURY

Department of the Treasury Appendix for FY 2021 Annual Report

This appendix discusses the FY 2021 activities of the Department of the Treasury.

Treasury IP-related efforts on Customs

Treasury authority for border enforcement of intellectual property laws, along with certain other customs revenue functions, has been delegated to DHS and is carried out by CBP and ICE (see Treasury Order 100-16 and 6 U.S.C. §§ 212, 215). Under the delegation, Treasury retains the sole authority to approve any regulations concerning copyright and trademark enforcement at the border and works closely on these promulgations with DHS and its components.

Treasury efforts to identify and address certain IP-related risks to national security through the CFIUS process

The Secretary of the Treasury serves as Chairperson of the Committee on Foreign Investment in the United States (CFIUS). CFIUS is an interagency committee authorized to review certain transactions that could result in control by a foreign person over a U.S. business in order to determine the effect of such transactions on the national security of the United States. Pursuant to the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which was signed into law on August 13, 2018, and subject to its implementing regulations, CFIUS also has the authority, among others, to review certain non-controlling investments by foreign persons in U.S. businesses that produce, design, test, manufacture, fabricate, or develop critical technologies, and this review may include aspects of a technology's underlying intellectual property. The Department of the Treasury continues to accept declarations and notices under its regulations implementing FIRRMA.

Among other things, these regulations mandate the filing of a declaration with CFIUS for certain foreign investment transactions involving a U.S. business that produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies based on whether certain U.S. Government export control authorizations would be required to export, re-export, transfer (in country), or retransfer such U.S. business's critical technology to certain transaction parties or their owners.

CFIUS does not enforce intellectual property laws. If, however, during its review of a transaction CFIUS identifies a risk to U.S. national security arising from a foreign person's acquisition of, or access to, the intellectual property of a U.S. business, and if other authorities are not adequate or appropriate to address the identified risk, CFIUS will seek to mitigate such risk. Mitigation measures could take a variety of forms, including but not limited to placing the intellectual property in escrow; controlling the foreign person's access to the intellectual property; requiring mechanisms to monitor and enforce such access controls; and ensuring U.S. Government access to, or insight into, the intellectual property. If CFIUS determines that the identified risk cannot be resolved through mitigation, CFIUS may refer the transaction to the President, who can, in accordance with section 721 of the Defense Production Act of 1950, as

amended, suspend or prohibit certain transactions that threaten to impair the national security of the United States.

Treasury authority to impose sanctions under Executive Order 13694, as amended, in response to certain malicious cyber-enabled activities, including the theft of trade secrets for commercial or competitive advantage or private financial gain.

Treasury continues to encourage referrals from relevant departments and agencies, including law enforcement and intelligence agencies, regarding targets for potential designation by the Office of Foreign Assets Control (OFAC) pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757. The Executive Order authorizes the imposition of sanctions on individuals and entities determined to be responsible for or complicit in, or to have engaged in, certain malicious cyber-enabled activities, including those “causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.”

**OFFICE OF THE UNITED STATES TRADE
REPRESENTATIVE**

OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE

USTR Appendix for FY 2021 Annual Report

This appendix discusses the FY 2021 activities of the Office of the U.S. Trade Representative.

One avenue to promote intellectual property (IP) protection and enforcement abroad is through engagement with our trading partners. Through such engagement, the Administration advocates for strong IP protection and enforcement in other countries for, *inter alia*, creative works, brands, designs, trade secrets, and inventions by U.S. creators, inventors, artists, and businesses. Through direct engagement with foreign counterparts, the Office of the U.S. Trade Representative (USTR) emphasizes the importance that the U.S. government places on protecting and enforcing IP, and presses for concrete action by trading partners to protect and enforce IP rights, including those owned by Americans.

To advance the Administration's objectives, USTR uses a broad range of trade policy tools to promote strong IP rights protection and enforcement, including Section 301 of the Trade Act; the annual Special 301 review of IP protection and enforcement and related market access issues; trade agreement negotiations; monitoring and enforcement of those agreements; trade and investment framework agreements; participation in the TRIPS Council at the World Trade Organization; and high-level engagement in multilateral and bilateral meetings.

Given the international competitiveness of U.S. innovative and creative industries, the United States considers strong and effective protection and enforcement of IP rights as critical to U.S. economic growth and American jobs. According to the U.S. Department of Commerce, 45.5 million American jobs in 2014 were directly or indirectly supported by "IP-intensive" industries, and these jobs paid higher wages to their workers. In addition, in 2014, these IP-intensive industries accounted for \$6.6 trillion in value added and 38.2 percent of the U.S. GDP. (See Department of Commerce, *Intellectual Property and the U.S. Economy: 2016 Update*, at <https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf>.) Innovation and creativity are key export strengths for the United States. Combatting unfair IP trade policies will encourage domestic investment in the United States, foster American innovation and creativity, and increase economic security for American workers and families.

The USTR initiatives that have advanced IP protection and enforcement include the following.

Section 301 Investigation into China's Technology Transfer, Intellectual Property and Innovation Law, Policies, Practices and Actions

On August 14, 2017, the President of the United States issued a Memorandum instructing the Trade Representative to determine whether to investigate under section 301 of the Trade Act of 1974 (the Trade Act) (19 U.S.C. § 2411) laws, policies, practices, or actions of the government of China that may be unreasonable or discriminatory and that may be harming American IP rights, innovation, or technology development. See 82 FR 39007. After consultation with the appropriate advisory committees and the interagency Section 301 Committee, on August 18, 2017, USTR initiated an investigation into certain acts, policies, and practices of China related to

technology transfer, IP, and innovation. See 82 FR 40213. The investigation included a public hearing on October 10, 2017, and two rounds of public written comments from interested members of the public.

On March 22, 2018, based on the investigation in response to the Presidential Memorandum, the Trade Representative issued a detailed report determining that China's acts, policies, and practices that force or pressure U.S. rightsholders to transfer technology and IP are unreasonable or discriminatory and burden or restrict U.S. commerce, and are thus actionable under Section 301(b) of the Trade Act. In a notice published in the *Federal Register* on April 6, 2018, the Trade Representative found:

- China uses foreign ownership restrictions, such as joint venture requirements and foreign equity limitations, and various administrative review and licensing processes, to require or pressure technology transfer from U.S. companies;
- China's regime of technology regulations forces U.S. companies seeking to license technologies to Chinese entities to do so on non-market-based terms that favor Chinese recipients;
- China directs and unfairly facilitates the systematic investment in, and acquisition of, U.S. companies and assets by Chinese companies to obtain cutting-edge technologies and intellectual property and generate the transfer of technology to Chinese companies; and
- China conducts and supports unauthorized intrusions into, and theft from, the computer networks of U.S. companies to access their sensitive commercial information and trade secrets.

The President directed the Trade Representative to take all appropriate action under Section 301, including considering increased tariffs on goods from China.

On April 6, 2018, USTR published a proposed list of products imported from China, worth approximately \$50 billion in imports that could be subject to additional tariffs. After hearings and the receipt of numerous written comments, the USTR imposed additional tariffs of 25 percent on approximately \$34 billion worth of imports from China, effective July 6, 2018. After a subsequent round of hearings and submissions, the USTR imposed additional tariffs of 25 percent on approximately \$16 billion worth of imports from China, effective August 23, 2018.

On September 24, 2018, USTR announced the imposition of additional tariffs of 10 percent on approximately \$200 billion worth of imports from China, which were later increased to a rate of 25 percent effective January 1, 2019. At the direction of the President, the Trade Representative initially postponed the rate increase for the additional tariff on this third tranche of products in light of progress in discussions with China, but on May 10, 2019, increased the rate to 25 percent after China retreated from specific commitments from earlier rounds of negotiations. In May 2019, USTR requested public comment and, in June 2019, held a public hearing on a proposed tariff modification imposing additional tariffs of up to 25 percent on approximately \$300 billion worth of imports from China.

On November 20, 2018, USTR released an update regarding its Section 301 investigation of China's acts, policies and practices related to technology transfer, IP and innovation.¹⁴ The update concluded that China had not fundamentally altered its acts, policies, and practices related to technology transfer, IP, and innovation that were the subject of the March 2018 report, and appeared to have taken further unreasonable actions in recent months.¹⁵

On March 23, 2018, the United States requested consultations with China under the WTO Dispute Resolution Understanding (in matter DS542). Consultations on DS542 were held in July 2018 but they did not resolve the dispute. On October 18, 2018, the United States requested that the WTO Dispute Settlement Body establish a panel to examine the U.S. complaint. After China blocked the first U.S. request for a WTO dispute settlement panel as provided for in the rules for dispute settlement proceedings, the United States repeated its request to establish a WTO dispute settlement panel and a panel was established at the November 21, 2018 meeting of the Dispute Settlement Body. In March 2019, China revised the measures that the United States had challenged. The United States considered that China's actions had sufficiently addressed U.S. concerns, and after 12 months, the authority of the panel expired on June 8, 2021.

In August 2019, the Trade Representative, at the direction of the President, determined to modify the action being taken in the investigation by issuing a notice imposing additional tariffs of 15 percent on \$120 billion worth of imports from China effective September 1, 2019, and additional tariffs of 15 percent on \$160 billion worth of imports from China effective December 15, 2019. The Trade Representative also received public comments regarding a proposed modification to increase the rate of additional duties from 25 percent to 30 percent on imports from China covered by the three prior tariff actions, with an approximate annual trade value of \$250 billion.

On January 15, 2020, the United States and China signed the Economic and Trade Agreement between Government of the United States of American and the Government of the People's Republic of China (the "Phase One Agreement"), which requires, *inter alia*, structural reforms and other changes to China's economic and trade regime in the areas of IP, technology transfer, agriculture, financial services, and currency and foreign exchange. In light of progress in the negotiations with China, and at the direction of the President, the Trade Representative determined to suspend indefinitely the imposition of the additional duties of 15 percent on \$160 billion worth of imports from China that had been scheduled for December 15, 2019. In addition, on February 14, 2020, the United States reduced from 15 percent to 7.5 percent the tariffs that had been imposed on September 1, 2019, on \$120 billion worth of goods from China.

Since the Phase One Agreement entered into force on February 14, 2020, the United States has been closely monitoring China's progress in implementing its commitments. The United States has also been fully utilizing the consultation arrangements set forth in the agreement for ensuring that China adheres to its obligations, including regular meetings required by the agreement between the two sides at the working level, the Deputy level and the Principal level. The two sides have also held numerous technical-level meetings. Through these many engagements, the United States has been able to raise and discuss with China any concerns that have arisen

¹⁴ <https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf>

¹⁵ *Id.*

regarding China's implementation progress, and the two sides have generally been able to work through them in a constructive manner.

The United States, Mexico, and Canada Agreement (USMCA)

The United State-Mexico-Canada Agreement (USMCA) entered into force on July 1, 2020. The USMCA will support mutually beneficial trade leading to freer markets, fairer trade, and robust economic growth in North America. It includes a modernized, high-standard IP chapter, which breaks new ground in U.S. trade and IP policy. It contains comprehensive protections against misappropriation of trade secrets, including by state-owned enterprises. It provides the most robust border enforcement mechanisms of any prior FTA. In addition, strong copyright protection and enforcement, more transparency in the grant of geographical indications (GI) protection or recognition, and full national treatment also promote the strong and effective protection and enforcement of IP rights that is critical to driving innovation, creating economic growth, and supporting American jobs.¹⁶

In April 2021, the USMCA Committee on Intellectual Property Rights met to discuss resources, education, and programs that are available in Canada, Mexico, and the United States that help micro, small, and medium-sized enterprises address issues such as IP infringement. The United States continues to engage with Canada and Mexico to ensure full implementation of the IP protection and enforcement obligations.

New Trade Negotiations

The United States and the UK launched trade negotiations in May 2020 under the prior administration. After her confirmation in March 2021, United States Trade Representative Tai began a review of the status and objectives of the United States-UK Free Trade Agreement (FTA) to inform our next steps with the UK.

In July 2020, the United States and Kenya launched trade negotiations under the prior administration. Through two negotiating rounds, the United States and Kenya discussed a range of issues related to an IP chapter. USTR is reviewing the status and objectives of the negotiations before deciding next steps.

Ongoing Trade Agreement Implementation and Enforcement

In FY 2021, the U.S. continued to engage with Free Trade Agreement (FTA) partners (including Australia, Chile, Colombia, and Costa Rica) to ensure that FTA obligations, including those related to IP, are being implemented.

¹⁶ United States–Mexico–Canada Trade Fact Sheet: Modernizing NAFTA into a 21st Century Trade Agreement (October 1, 2018) - <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/october/united-states%E2%80%93mexico%E2%80%93canada-trade-fa-1>

USTR Special 301 Report

Each year, pursuant to statute, USTR issues the Special 301 Report on the adequacy and effectiveness of protection and enforcement of IP by our trading partners. The Special 301 Report is an important tool to engage with our trading partners to promote strong protection for U.S. creative and innovative industries, as well as to promote compliance with trade commitments. USTR actively employs the Special 301 process to identify and address key IP challenges for American businesses and to document and encourage continued progress in countries that undertake legislative and enforcement reforms following engagement under Special 301.

USTR released the 2021 Special 301 Report in April 2021. (The 2021 Report is at [https://ustr.gov/sites/default/files/files/reports/2021/2021 Special 301 Report \(final\).pdf](https://ustr.gov/sites/default/files/files/reports/2021/2021%20Special%20301%20Report%20(final).pdf), and the related press release is at <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/april/ustr-releases-annual-special-301-report-intellectual-property-protection>.) In the report, USTR highlighted serious and ongoing concerns with respect to the environment for IP rights protection and enforcement in China, India, Indonesia, Russia, Saudi Arabia, Ukraine and other markets.

The Special 301 Report provides an opportunity to put a spotlight on foreign countries and the laws, policies, and practices that fail to provide adequate and effective IP protection and enforcement for U.S. inventors, creators, brands, manufacturers, and service providers, which, in turn, harm American workers whose livelihoods are tied to America's innovation-driven sectors. The Report identifies a wide range of concerns, including (a) challenges with border and criminal enforcement against counterfeits, including in the online environment; (b) high levels of online and broadcast piracy, including through illicit streaming devices; (c) inadequacies in trade secret protection and enforcement in China, Russia, and elsewhere; (d) troubling "indigenous innovation" and forced technology transfer policies that may unfairly disadvantage U.S. rightsholders in markets abroad; and (e) other ongoing, systemic issues regarding IP protection and enforcement, as well as market access, in many trading partners around the world. Combatting such unfair trade policies will encourage domestic investment in the United States, foster American innovation and creativity, and increase economic security for American workers and families.

Notorious Markets List

The Notorious Markets List (NML) highlights select online and physical marketplaces that reportedly engage in or facilitate substantial copyright piracy or trademark counterfeiting. USTR has identified notorious markets in the Special 301 Report since 2006. In 2010, USTR announced that it would begin publishing the NML separately from the annual Special 301 Report, pursuant to an Out-of-Cycle Review. USTR first separately published the 2010 NML in February 2011, and has published an NML for every year since.

In the NML, USTR highlights markets not only because they exemplify global concerns about counterfeiting and piracy, but also because the scale of infringing activity in such markets can cause significant economic harm to U.S. IP rightsholders. Some of the identified markets

reportedly are host to a combination of legitimate and unauthorized activities. Others reportedly exist solely to engage in or facilitate unauthorized activity. The NML does not purport to be an exhaustive list of all physical and online markets worldwide in which IP rights infringement takes place.

A goal of the NML is to motivate appropriate action by the private sector and governments to reduce piracy and counterfeiting. The operators of several websites identified in past NMLs have begun to work with rightsholders to address counterfeiting and piracy. Several markets have also ceased operations or have been the focus of government enforcement efforts.

The 2020 Notorious Markets List was issued in January 2021. (The NML is at [https://ustr.gov/sites/default/files/files/Press/Releases/2020_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy_\(final\).pdf](https://ustr.gov/sites/default/files/files/Press/Releases/2020_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy_(final).pdf), and the related press release is at <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/january/ustr-releases-2020-review-notorious-markets-counterfeiting-and-piracy>.) The 2020 NML includes a focus that explores e-commerce and the role of internet platforms in facilitating the importation of counterfeit and pirated goods into the United States.

India

The U.S. maintains bilateral engagement with India on IP issues through the High-Level IP Working Group under the United States–India Trade Policy Forum (TPF). USTR, working with its interagency partners (USPTO, U.S. Copyright Office, ITA, DOJ, Health and Human Services, FTC, and others), revitalized on-going engagement with Indian government counterparts during FY 2021, including IP Working Group meetings held in December 2020, and June and August 2021, and continued exchanges and activities centered on the robust protection of IP and enforcement of IP rights, with a focus on areas such as copyright, trade secrets, patents, and promoting innovation and creativity through high-level government policies.

World Trade Organization Council on Trade-Related Aspects of Intellectual Property Rights (TRIPS Council)

The World Trade Organization (WTO) provides an additional venue for USTR to lead engagement with trading partners on IP rights issues, including through accession negotiations for prospective Members, the Council for Trade-Related Aspects of Intellectual Property Rights (TRIPS Council), and the Dispute Settlement Body.

In FY 2021, the United States advanced its IP and Innovation agenda in the TRIPS Council by focusing on intellectual property and innovation in connection with the development of micro, small and medium enterprises (MSMEs). The United States is working with WTO Members including Australia, Canada, Chile, Chinese Taipei, the European Union, Japan, Hong Kong, Russia, Singapore, South Korea, Switzerland, New Zealand, and the United Kingdom, examining how IP protection and enforcement promote innovation and creativity to meet societal challenges and needs.

World Trade Organization Accession

Governments in the process of negotiating the terms for accession to the WTO work with WTO Members, including the United States, to appropriately update and strengthen their IP regimes as well as to expand trade and enhance the investment climate for innovative and creative industries.

Other Fora

In addition to the WTO (which is the principal forum for addressing trade-related aspects of intellectual property), the United States also advanced these issues in other fora during FY 2021, including the OECD, WIPO, APEC forum, and various U.N. bodies.

In the APEC Intellectual Property Experts Group (IPEG), the United States is continuing a series of workshops for IPEG members on the importance of industrial design protection and how developing modern design protections across APEC economies will promote economic growth. In addition, to build upon a survey issued by the United States for IPEG members on treatment of, and approaches to, illicit streaming devices (ISDs) under domestic laws or regulations, the United States published the *Report on Results of Survey Questionnaire on Domestic Treatment of Illicit Streaming* and hosted a webinar on *Content Protection and Illicit Streaming: Enforcement Approaches and Strategies*. The United States also proposed an effective practices document for enforcement against illegal streaming, with the goal of obtaining APEC endorsement.

Examples of Additional Areas of IP Rights Engagement

In FY 2021, Ukraine's CMO system remained a work in progress and a source of concern in terms of implementing a transparent, fair, and predictable collective management regime, despite Ukraine taking some positive steps on this issue. USTR, coordinating with interagency subject matter experts, also engaged with Ukrainian counterparts on next steps for addressing longstanding concerns such as online piracy and government use of unlicensed software, including through the TIC's Intellectual Property Rights Working Group.

USTR has been engaging with the government of South Africa in 2021 on copyright policy and other intellectual property protection issues including on its open review of South Africa's eligibility for the GSP program. USTR opened the review after accepting a petition from the International Intellectual Property Alliance (IIPA) asserting that South Africa is not providing adequate and effective copyright protection and that, if South Africa enacts two pending copyright bills, it will move even further from international norms. In June 2020, the president of South Africa had sent back to Parliament those two copyright bills, and, in June 2021, Parliament rescinded both bills. Legal authorization for the benefits under the GSP program expired on January 1, 2021. As long as GSP remains without authorization, the USTR does not intend to hold public hearings, open new country eligibility reviews, or move toward final determinations of our ongoing reviews.

The Central Asia IP Working Group serves as an important mechanism to provide sustained engagement on IP issues and help improve IP regimes in the region. The Working Group met virtually in January and July 2021, and at a United States-Central Asia TIFA Council meeting held in late March and early April 2021.

In June 2021, the United States and Taiwan held a TIFA Council meeting under the auspices of the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO). The two sides recognized progress that has been made, such as Taiwan's enforcement of trade secrets protections, and committed to intensify engagement aimed at addressing outstanding trade concerns, including with regard to concerns raised by the U.S. in areas such as copyright legislation and digital piracy.

The United States held a TIFA intersessional meeting with Pakistan in December 2020 and TIFA Council meetings with Nepal in December 2020, Fiji in February 2021, and Uruguay in August 2021. The United States also held a technical meeting under the U.S.-Thailand TIFA in October 2020; the U.S.-Paraguay TIFA in December 2020 and subsequent technical meetings; the U.S.-Indonesia TIFA in September 2021; IP Working Group meetings under the United States-Kuwait TIFA in May and September 2021; a Trade Dialogue on IP protection and enforcement with the United Arab Emirates in June 2021; and an Innovation and Creativity Forum with Argentina in November 2020. These meetings discussed a range of issues relating to IP protection and enforcement, such as combatting the sale of counterfeit and pirated goods.

Engagement with Stakeholders and the Public

USTR frequently seeks public input from all sectors of society, including private citizens, non-governmental organizations, academia, consumer groups, small and medium-size businesses, and the business community (including innovators, content providers, and technology and other service providers).

To this end, USTR holds public hearings; seeks written comments regarding negotiation objectives through *Federal Register* notices; chairs regular sessions with designated public advisory committees; and disseminates trade policy materials such as press releases, factsheets, and statements on the USTR website. These dialogues are critical at every stage of USTR's work, including in connection with the process of negotiating, implementing, and enforcing trade rules.

USTR also seeks public input for the annual Special 301 and Notorious Markets List processes. The annual Special 301 Report identifies countries that fail to adequately and effectively protect or enforce IP rights or use unfair barriers to limit market access for U.S. businesses that rely on IP. The Notorious Markets List highlights prominent online and physical marketplaces that reportedly engage in or facilitate substantial copyright piracy or trademark counterfeiting. USTR publishes requests for public comment in the *Federal Register* that provide opportunities for public input and rebuttals, and the submitted comments are available online. In addition, USTR holds a public hearing for the Special 301 process.¹⁷ In addition to requesting comments from the public and

¹⁷ In 2021, due to COVID-19, USTR fostered public participation via written submissions rather than an in-person hearing with the interagency Special 301 Subcommittee of the Trade Policy Staff Committee (TPSC) sending

holding a public hearing on IP matters, IP trade policy figured heavily in USTR's broader stakeholder and Congressional outreach, including in a range of domestic and international fora.

written questions about issues relevant to the review to those that submitted written comments, including to representatives of foreign governments, industry, and non-governmental organizations.

COPYRIGHT OFFICE

COPYRIGHT OFFICE

Copyright Office Appendix for FY 2021 Annual Report

This appendix summarizes some of the key enforcement-related activities taken by the United States Copyright Office in FY 2021.

Overview

During FY 2021, the Office continued to work on a breadth of copyright-related issues, including the implementation of the Orrin G. Hatch-Bob Goodlatte Music Modernization Act (MMA); the creation of the Copyright Claims Board (CCB) pursuant to the Copyright Alternative in Small-Claims Enforcement Act of 2020 (CASE Act); several policy studies; and efforts to modernize the Office's operations. The Office also provided law and policy advice to Congress, provided expert advice to the federal courts and executive branch agencies on domestic and international copyright matters, and conducted public outreach and education efforts. Please visit <https://www.copyright.gov/> for more information on all of the Office's activities.

Reports & Studies for Congress

The Copyright Office advises Congress on national and international issues relating to copyright. 17 U.S.C. § 701(b)(1). This advice includes providing requested opinions on pending and existing legislation as well as providing analyses on areas of copyright law. The Office seeks to ensure that all members of the copyright community – including copyright owners, technology companies, consumers, public interest groups, academics, and the general public – have robust opportunities to participate and contribute to the Office's policy studies, reports, and recommendations.

During FY 2021, the Office completed two studies related to enforcement, one analyzing copyright owner remedies for state infringement and another recommending best practices to ensure copyright owners receive payment for works used by digital service providers.

State Sovereign Immunity Study

In response to the Supreme Court's ruling in *Allen v. Cooper*, Senators Thom Tillis and Patrick Leahy sent a letter to the Copyright Office on April 28, 2020, asking the Office to commence a public study to discover the degree to which copyright owners are experiencing copyright infringement by states without adequate remedies under state law (<https://www.copyright.gov/policy/state-sovereign-immunity/letter.pdf>).

In its March 2020 ruling in *Allen v. Cooper*, the Supreme Court held that Congress exceeded its constitutional authority when it enacted legislation (the Copyright Remedy Clarification Act of 1990) that authorized copyright infringement suits to be brought against states for damages. Relying on the Court's prior decision in *Florida Prepaid Postsecondary Ed. Expense Bd. v. College Savings Bank* (1999), which addressed a 1992 statute that sought to abrogate state sovereign immunity from patent-infringement suits, the Court in *Allen v. Cooper* stated that

“*Florida Prepaid* all but rewrote our decision today. That precedent made clear that Article I’s Intellectual Property Clause could not provide the basis for an abrogation of sovereign immunity. And it held that Section 5 of the Fourteenth Amendment could not support an abrogation on a legislative record like the one here.” With respect to its conclusion that the legislative record for the 1990 copyright statute could not support its abrogation of state sovereign immunity, the Court explained that this conclusion “need not prevent Congress from passing a valid copyright abrogation law in the future,” stating that – in enacting the 1990 statute – “Congress likely did not appreciate the importance of linking the scope of its abrogation to the redress or prevention of unconstitutional injuries—and of creating a legislative record to back up that connection. But going forward, Congress will know those rules. And under them, if it detects violations of due process, then it may enact a proportionate response.”

To commence the study, the Copyright Office issued a notice of inquiry requesting comments on issues, such as specific instances of infringement committed by states, whether the infringement was intentional or reckless, and the availability of remedies under state law. The Office held public roundtables for this study via Zoom and also accepted additional public comments and evidence from participants of the roundtable discussions who were not able to speak or submit materials during the event. The Office found that the evidence submitted indicates that state infringement represents a legitimate concern for copyright owners. However, the Office could not conclude with certainty that the record would be found sufficient to meet the constitutional test for abrogation.

The full report, public comments, recordings and transcripts of the roundtables, and additional materials submitted after the roundtable event can be found at <https://www.copyright.gov/policy/state-sovereign-immunity/>.

Unclaimed Royalties Study

In connection with the MMA, the newly designated Mechanical Licensing Collective (“MLC”) is tasked with administering the new blanket license under section 115 of the Copyright Act; distributing royalties to songwriters and music publishers; and, among other duties, implementing policies and procedures for distributing unclaimed accrued royalties and interest after a prescribed holding period. As directed by the MMA, and in consultation with the Government Accountability Office, the Copyright Office undertook a study to recommend best practices that the MLC may implement to identify and locate musical work copyright owners with unclaimed royalties, encourage those copyright owners to claim their royalties, and ultimately reduce the incidence of unclaimed royalties. Prior to FY 2021, the Office held a symposium featuring educational discussions of the issues; commissioned a report addressing global collective management organizations’ approaches to obtaining ownership information, reducing the instance of unclaimed royalties and royalty distribution; and issued a notice of inquiry seeking public comments for the report. During FY 2021, the Office held public roundtables and received materials from roundtable participants who wished to share additional information during the event but were unable to do so.

The report recommends that the MLC should:

- engage, to the broadest extent reasonably possible, in conducting education and outreach activities;
- make sure that its public facing systems or services are simple, accessible, well-organized, and user-friendly, with flexible and robust tools, features, and functionality across multiple platforms;
- take reasonable steps to ensure that its data is of the highest possible quality;
- employ both automated and manual matching processes that rely on standard unique identifiers;
- adopt transparent, practical, and equitable policies, practices, and procedures, especially with respect to holding and distributing unclaimed royalties;
- closely monitor and track a wide variety of metrics and continually review and analyze them to evaluate its level of success and relative effectiveness over time; and
- be transparent about its activities and continue to engage regularly with stakeholders.

The full report as well as public comments, the notice of inquiry, the symposium materials, and materials from the public roundtables are available at <https://www.copyright.gov/policy/unclaimed-royalties/>.

Rulemakings

During FY 2021, the Copyright Office engaged in a number of additional rulemakings. A list of both open and closed rulemakings is available at <https://www.copyright.gov/rulemaking/>. An illustrative list of enforcement-related rulemakings appears below.

MMA Rulemakings

The MMA was enacted in October 2018 and addressed licensing to ensure music streaming services, or digital service providers, do not infringe copyright in the operation of their services. The MMA requires, among other things, that the Copyright Office adopt several regulations to govern the new blanket licensing system created under Title I of the MMA, known as the Musical Works Modernization Act. The blanket licensing system replaces the existing song-by-song compulsory licensing structure for making and distributing musical works with a blanket licensing system for digital music providers to make and distribute digital phonorecord deliveries (e.g., permanent downloads, limited downloads, or interactive streams). The blanket licensing system became available January 1, 2021.

In FY 2021, the Office continued rulemakings under the MMA, issuing three interim rules and one final rule. The first interim rule addresses a variety of reporting obligations between blanket

licensees or significant nonblanket licensees and the Mechanical Licensing Collective (MLC). The second interim rule prescribes the categories of information to be included in the public musical works database and rules related to the usability, interoperability, and usage restrictions of the database. The third interim rule creates various restrictions on the disclosure and use of confidential information by the MLC and digital licensee coordinator (DLC), as well as their employees, agents, consultants, vendors, independent contractors, and members of their board of directors and committees. The final rule addresses cumulative statements of account required to be submitted by digital music providers to the MLC for such providers to be eligible for the statutory limitation on liability for unlicensed uses of musical works prior to the January 1, 2021 license availability date.

For more on the MMA and the Office’s implementation of this act, *see* <https://www.copyright.gov/music-modernization/>.

CASE Act and the Copyright Claims Board

In December 2020, Congress enacted the Copyright Alternative in Small-Claims Enforcement Act of 2020 (CASE Act) to establish a new Copyright Claims Board (CCB) that would be a voluntary “small copyright claims” tribunal comprised of three Copyright Claims Officers who will have the authority to render determinations on certain copyright claims of low financial value. The CASE Act directs the Office to adopt several regulations to govern the CCB and its procedures. The statute further vests the Office with general authority to adopt such regulations as may be necessary or appropriate to effectuate the Board.

To assist in promulgating these regulations, the Office sought public comment and completed a rulemaking proceeding to establish procedures for a new expedited registration option for works at issue before the CCB. The rule enables a claimant or counterclaimant with a pending copyright registration application to seek expedited review of that application. The CCB cannot proceed with a dispute involving a work for which registration is still pending or has been denied. The Office also issued a notice of proposed rulemaking to address procedures for libraries and archives to preemptively opt out of proceedings before the CCB and to propose procedures related to federal court class action proceedings for a party who is before the Board. This rulemaking will continue into FY 2022. The Office plans on publishing additional CASE Act notices of proposed rulemaking and final rules before the Copyright Claims Board begins operations.

All CASE Act-related rulemakings can be found at <https://copyright.gov/rulemaking/case-act-implementation/>. Additional information on the CASE Act can be found here: <https://copyright.gov/about/small-claims/>.

Recordation and Notices of Termination

Notices of termination are a mechanism by which authors or their heirs, under certain circumstances, can terminate the exclusive or nonexclusive grant of a transfer or license of an author’s copyright in a work or of any of the exclusive rights under a copyright. The Copyright Office issued amendments to its regulations governing recordation of notices of termination

under sections 203 and 304(c) of the Copyright Act. In addition, the Office announced changes to its examination practices for certain notices of termination that pertain to multiple grants. The changes relate to regulatory provisions governing timeliness, harmless errors, manner of service, and the date of recordation for notices of termination. These amendments are intended to improve efficiency in the processing of notices in conjunction with the development of the Office's online electronic recordation system.

International Activities

Throughout the year, the Copyright Office continued to provide outreach and education regarding copyright issues to foreign officials via video meetings. The Office also hosted international programs to discuss and exchange information on the U.S. copyright system and significant international copyright issues. The Office works with other agencies, including the State Department, the Office of the U.S. Trade Representative (USTR), and the U.S. Patent and Trademark Office (USPTO), to participate in meetings affecting international policy decisions on intellectual property enforcement and other IP topics.

Advise Executive Branch Agencies on International Copyright & Trade Matters

The Copyright Office supports USTR and other executive branch agencies by serving on official delegations and negotiating teams, as part of its statutory duties (17 U.S.C § 701(b)). In FY 2021, the Office supported the U.S. government delegations to the World Intellectual Property Organization (WIPO) where the Standing Committee on Copyright and Related Rights (SCCR) has been discussing, among other topics, a draft treaty that would protect broadcasting organizations against signal piracy.

The Office also participated in the annual Special 301 review facilitated by USTR, including the Notorious Markets out-of-cycle review, and engaged in regular consultation with executive branch agencies on copyright law and enforcement developments in other countries, including draft legislation and guidance documents, compliance efforts, World Trade Organization trade policy reviews and accessions, the proposed Trade-Related Aspects of Intellectual Property Rights waiver, and reviews under trade preference programs.

International Copyright Institute

Every two years, the Copyright Office and WIPO co-host the International Copyright Institute, a week-long program designed to provide representatives from developing countries and countries in transition with a deeper understanding of copyright law in the digital age. Participants learn about a range of topics, including new distribution models for digital content, modern copyright registration systems, and enforcement challenges. Due to the COVID-19 pandemic, the International Copyright Institute was postponed a year and held in a condensed and virtual format in July 2021. The two-day program, *New Copyright Developments in the United States of America and Internationally*, invited participants from twenty-four countries to discuss topical and emerging issues in the field of copyright that are taking place in the U.S. and internationally, including the Music Modernization Act and CASE Act, the rapidly changing digital environment, and the global impact of the pandemic on copyright.

Copyright Office Modernization

Over the past several years, the Copyright Office has engaged in several modernization efforts to provide a more user-centered and flexible design for the Office’s electronic registration, recordation, and public record work streams, along with modernizing the Office’s information technology (IT) support systems. More information about the Office’s modernization efforts can be found at <https://www.copyright.gov/copyright-modernization/>. The Office also hosts a bimonthly webinar series that focuses on various aspects of the modernization process. All webinars can be found at <https://www.copyright.gov/copyright-modernization/webinar/>.

Copyright Public Modernization Committee

The Library of Congress established a new Copyright Public Modernization Committee (CPMC) to expand and enhance communication with external stakeholders on IT modernization of Copyright Office Systems. Committee members were selected by the Librarian from a pool of applicants for their ability to represent a broad cross section of the copyright community and other interested groups. The committee will meet twice a year through 2024 to publicly share information and answer questions about the IT-related aspects of Copyright Office modernization. A list of the CPMC members is available at <https://www.copyright.gov/newsnet/2021/898.html>.

Circular 92 Update

Being able to access the current law is important for copyright owners to know how to enforce their rights. The Copyright Office released an updated version of *Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code* in both online and physical versions. Also known as Circular 92, this publication contains the text of the Copyright Act, including all amendments enacted by Congress through December 27, 2020, including the CASE Act of 2020.

Fair Use Index

The Copyright Office hosts and maintains the Fair Use Index, which was undertaken in coordination with the Intellectual Property Enforcement Coordinator. This searchable database contains notable cases from U.S. courts that comment on fair use law. The Index contains more than 200 cases. The Office continually updates the Index to keep practitioners and the public informed of new or prominent issues in fair use law, the application of fair use to a variety of types of works, and the law across appellate jurisdictions in the United States. The Index contains clear and concise language describing the facts and outcome of each case, making the Index accessible to the general public and providing valuable information—including a full legal citation—to aid a viewer in further research. The Fair Use Index is hosted at <https://www.copyright.gov/fair-use/>.

Public Outreach

The Copyright Office implements a full program of outreach activities to educate the public regarding copyright protections. The Office's outreach programs cover a wide range of formats and media, including live presentations, video tutorials, social media, and participation in programs hosted by outside organizations. Illustrative examples include the following.

Public events: In April 2021, the Copyright Office celebrated World Intellectual Property Day with a program, *The Creative Business: Celebrating World IP Day and Taking Your Ideas to Market*, which reflects the World Intellectual Property Organization's 2021 theme. This event featured a discussion of the importance of small and medium businesses in copyright, the economy, and our culture. Panelists provided insights into how to navigate copyright issues that are unique to small and medium businesses. The Office also hosted a virtual event celebrating the enduring copyright legacy of Justice Ruth Bader Ginsburg.

Legal audience events: The Copyright Office, in conjunction with the Georgetown Intellectual Property and Information Policy Clinic and Georgetown Institute for Law and Policy Online, hosted a discussion on the legacy of former Register Barbara Ringer and the importance of creating space and opportunities in copyright and developing more diverse and inclusive legal systems for the benefit of all. The Register of Copyrights and senior staff also spoke on a wider number of issues at several events with legal audiences (such as the American Bar Association, the International Trademark Association (INTA), and the Copyright Society) and at other legal and academic events.

Outreach for Creators: The Copyright Office published *How Songwriters, Composers, and Performers Get Paid*, a guide breaking down different music royalty streams and the importance of copyright. The Copyright Office participated in the Imaging USA (IUSA) photography conference, answering photographers' questions about copyright and enforcement. The Copyright Office launched a new webpage to help the music community understand copyright principles, including the various types of works, registration, how to use others' works, infringement, and important laws affecting the music community.