CONGRESSIONAL REPORT
FEDERAL BUREAU of INVESTIGATION
PRO IP ACT ANNUAL REPORT
2011

The Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO IP Act) authorized appropriations for personnel and operational enhancements for the FBI. In accordance with the guidance in the PRO IP Act, the FBI provided an initial report in October 2009 summarizing its efforts, activities, and resources allocated in the five years prior to the date of enactment as well as its efforts, activities, and resources allocated in the first year following the date of enactment. The FBI then provided an Annual Report for Fiscal Year (FY) 2010 in accordance with the guidance in the PRO IP Act to provide subsequent annual reports detailing its actions taken in furtherance of carrying out the title. This report serves as the third annual report, and summarizes the efforts, activities, and resources allocated in FY 2011.

Executive Summary

The FBI's overall strategy for Intellectual Property Rights (IPR) enforcement is to disrupt and dismantle international and domestic criminal organizations and individuals that manufacture or traffic in counterfeit and pirated goods and/or steal, distribute or otherwise profit from the theft of intellectual property. Investigative priorities include theft of trade secrets, counterfeit goods that pose a threat to health and safety, and copyright and trademark infringement cases having a national security, organized crime, or significant economic impact.

The FBI is a full and active partner at the National Intellectual Property Rights Coordination Center (IPR Center). The IPR Center serves as a centralized, multiagency entity to coordinate, manage, and advocate the U. S. Government's Federal criminal enforcement of intellectual property rights laws.

The FBI aggressively pursues intellectual property enforcement through its role at the IPR Center, traditional investigative methods in the field and at the IPR Center, intelligence driven initiatives, and through coordinated efforts with both private industry and domestic and foreign law enforcement partners.

As of 09/30/2011, the FBI had 499 pending IP investigations:

- 100 theft of trade secret
- 85 copyright infringement (software)
- 141 copyright infringement (other than software)
- 54 trademark infringement
- 21 copyright infringement (signal theft)
- 24 counterfeit aircraft parts
- 22 counterfeit electrical parts

- 7 counterfeit automotive parts
- 45 counterfeit health products

The FBI had the following investigative accomplishments reported for FY 2011 as of 9/30/2011:

- 235 investigations initiated (236 new investigations
- 93 arrests
- 79 information/indictments
- 79 convictions

(Statistics regarding sentencing information, including statutory maximum and average sentences imposed for IPR-related crimes, are found in the Computer Crime and Intellectual Property Section, DOJ Congressional Report, 2011.)

The FY 2011 appropriations provided funds to support the IP enforcement mission of the FBI, specifically for personnel, equipment, training, and other critical support. As required, the FBI has placed all 51 IPR-dedicated agents, the majority of whom are placed in specified field offices with DOJ Computer Hacking and Intellectual Property (CHIP) units. In FY 2011, the actual direct IPR agent resources expended exceeded the required 51 agent-resources by 3.5 agent years, to 54.5. This resource commitment is separate from, and in addition to, those FBI agents assigned to investigate violations of the Economic Espionage Act, Title 18, Section 1831 as well as FBI agents working other criminal and national security matters that may have a tangential nexus to IPR. The FBI requested the assistance of digital forensic specialists, the Computer Analysis and Response Team (CART), on 128 occasions in support of IPR investigations.

PRO IP Act Personnel:

The FY 2009 Appropriations Bill provided for the "creation of an additional and distinct operational unit at FBI Headquarters with at least five full-time, permanent Special Agents (SAs) dedicated to working with the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) on complex, multi-district and international criminal IPR cases." Accordingly, the FBI established its Intellectual Property Rights Unit (IPRU) which is staffed with six SAs, two Management Program Analysts, one Staff Operations Specialist, and supported by Intelligence Analysts (IAs) from the Cyber Intelligence Section. In April, 2010, the FBI permanently located the IPRU at the IPR Center. The IPRU is led by a Unit Chief (UC), who also serves as a Deputy Director of the IPR Center. In addition to the UC, the IPRU also has two Supervisory Special Agents (SSAs) who provide strategic guidance, promote the development of intelligence, and manage the field office IPR programs. In addition, three SAs are assigned to the IPR Center to conduct complex, multi-district and international investigations. In addition, these SAs and IPRU personnel have been deployed to FBI field offices to "surge" on IPR investigations as needed. During FY 2011, two such deployments occurred.

This distribution of investigative resources maximizes the nationwide reach and ability of the FBI to detect and disrupt state sponsored groups and international and domestic criminal organizations that manufacture, distribute, and engage in IP crime. The disbursement also provides 22 of the 25 CHIP units with one or more SAs to work in direct support of IPR violations/prosecutions. With the concurrence of the Department of Justice, the remaining three field offices have an FBI IP Coordinator to support the CHIP units there. The IP Coordinator maintains regular contact with the CHIP units to ensure priority IP matters are supported fully. The locations for the distribution of these resources were selected based on a regional domain analysis of the threat to IP, field office statistics, IP threat intelligence reporting, input from the IPR CENTER, and an understanding that IPR violations and subject locations made it possible to establish venues regionally. The placement of the SAs was coordinated with and approved by the Office of the Deputy Attorney General and the Executive Office of the United States Attorneys (EOUSA) in FY 2010.

PRO IP Act Funding:

As part of FY 2011 appropriations, the FBI received personnel and non-personnel funding to support its IPR program. The use of that funding by the FY 2011 appropriations is provided below:

- Personnel funding - 51 dedicated IPR special agent positions assigned to field divisions contiguous to DOJ Computer Hacking and Intellectual Property (CHIP) Units and at FBIHQ/IPR Center,
- $703,134 in direct support of IPR investigations, to field divisions for the purchase of evidence, undercover operations, equipment, and supplies,
- $78,720 for selection and deployment of a dedicated IPR Agent to Beijing, China,
- $ 372,656 for domestic and international IPR training and related travel costs,
- $172,416 – for operational travel of field IPR agents and HQ components,
- $597,089 for contractor support as follows:
    - $167,878 for the IPR Center's Global Report on IPR Threats to the U.S.
    - $429,211 for expert computer forensic analysis and investigative support,
- $215,909 for development, hosting, and maintenance of the IPR Center's website, www.iprcenter.gov,
- $500,000 for forensic, investigative, and analytic software,
- $361,332 for CyD training facility build out,
- $200,000 for CyD project (Career Path Special Agent) training.

Efforts and Activities in Support of the FBI's IPR Program:

Investigative Case Highlights

The most important aspect of the FBI's IPR program is the investigation of high priority and high impact IPR matters and the successful prosecution thereof. In FY 2011 the FBI achieved significant success in this area. This included, among other things, new investigations, new undercover operations, and the execution of search warrants yielding critical evidence. The following are highlights of selected IPR investigations which were completed during FY 2011.

- The FBI conducted an investigation of a computer programmer employed at Goldman Sachs & Co. (Goldman Sachs). The defendant was responsible for developing computer programs to support the business's high-frequency trading. Goldman Sachs acquired this program in 1999 for approximately $500 million, modified and maintained it, and protected the technology as a trade secret. The defendant resigned from his job at Goldman Sachs to work for a competitor, and on his final day of employment transferred significant amounts of Goldman Sachs's proprietary computer code to an external computer server without informing or seeking approval from Goldman Sachs. Further investigation revealed the defendant had transferred thousands of proprietary computer code files from the firm's computers to his home computers without the knowledge of or authorization from Goldman Sachs. The defendant brought a laptop and an external storage device, both containing Goldman Sachs's proprietary computer code, to attend meetings at a competitor's firm where the defendant had secured new employment. In December 2010, the defendant was found guilty of theft of trade secrets and interstate transportation of stolen property. In March 2011, the defendant was sentenced to 97 months in prison, 3 years of supervised release following his prison sentence, and a $12,500 fine.

- The FBI initiated an investigation of an employee for the Ford Motor Company (Ford) who stole Ford trade secrets. The defendant accepted a job at a rival U.S. company located in China. Prior to leaving Ford's employment and without Ford's authorization or knowledge, the defendant copied approximately 4,000 sensitive Ford documents to an external hard drive, including proprietary design specifications for various engine and electrical systems. Ford spent millions of dollars and decades of man-hours on research, development, and testing of the systems in these documents. The defendant transported the sensitive Ford documents to his new employer, Beijing Automotive Company (BAC), in China. The FBI examined the defendant's official BAC laptop and identified 41 Ford system design specifications documents on the computer, and each of these documents had been accessed by the defendant during his employment with BAC. The defendant pleaded guilty to two counts of theft of trade secrets and was sentenced to 70 months in federal prison and a fine of $12,500 in April 2011.

- The FBI investigated a former trader at Société Générale ("SocGen") for theft of trade secrets. The defendant worked as a quantitative analyst and trader in SocGen's High Frequency Trading Group. SocGen developed a multi-million dollar computer system and code for high-speed trading, and took significant measures to protect this proprietary code from theft. The defendant had access to one portion of the code and printed hundreds of pages of it, taking the copies out of his office and transporting them to his residence without the knowledge or permission of SocGen. The defendant met with representatives from a rival trading group and provided them with SocGen's confidential proprietary code in order to secure a more profitable job at the competitor company. The defendant was found guilty in November 2010 of theft of trade secrets and interstate transportation of stolen property. In February 2011, he was sentenced to 36 months in prison and two years of supervised release.

- The FBI investigated four individuals for conspiracy, smuggling, and trafficking in counterfeit goods, specifically counterfeit Cisco computer hardware. The defendants owned and ran a Colorado-based company advertising products manufactured by Cisco that were "new in box" with their original packaging, yet offered the products at significantly lower prices than authorized Cisco distributors. The defendants purchased counterfeit Cisco products from unauthorized distributors in China, California, and Canada. The defendants also requested their suppliers include fraudulent or misleading shipping information on the packages in an attempt to smuggle the goods through customs. The defendants received separate shipments of empty counterfeit Cisco boxes and counterfeit product labels, which they in turn used to package the goods for their end users. One defendant pleaded guilty in March 2011, and two others pleaded guilty in May 2011. One defendant was ordered to pay federal restitution in the amount of $1,194,736.

- The FBI investigated RISCISO, a warez group involved in the illegal distribution of large volumes of copyrighted software, games, and movies via the Internet. The investigation led to the indictment of 19 individuals for conspiring to commit copyright infringement. Many of the illegally distributed items were recent releases, and all of the content was available to RISCISO members and affiliates. The total retail value of the software, movies, and games available for downloading on one server during its operation exceeded $6.5 million. At least seven defendants were sentenced in January and February 2011, most receiving sentences of 24-36 months probation, $2,000-15,000 fines, and 200 hours of community service.

- The FBI investigated members of "Old School Classics" ("OSC"), a warez group specializing in the unauthorized reproduction and distribution of copyrighted music using the Internet for over five years. OSC members were responsible for the early release of Kanye West's album "Graduation" in August 2007, more than one week before the album was commercially released. OSC received other pre-release music from two former members of "Rabid Neurosis" (RN), another warez group. The former RN members worked at a factory that manufactured compact discs for Universal Music

Group and its subsidiary labels, giving them access to music before its public release. The two RN members pleaded guilty to conspiracy to commit willful copyright infringement and were sentenced to three months in prison and two years of supervised release in January 2010. The leader of OSC pleaded guilty to conspiring to commit criminal copyright infringement in May 2011. In July 2011, the OSC leader was sentenced to 2 years probation, 6 months home detention, 100 hours of community service, and a $3,000 fine.

Domestic Liaison and Training

- The FBI is an original and key partner at the National IPR Center and fills a Deputy Director role there. The IPR Center, which is led by the U.S. Immigration and Customs Enforcement (ICE), Department of Homeland Security, brings together in a single location, the major U.S. agencies responsible for the enforcement of laws related to Intellectual Property crimes. The IPR Center optimizes the authorities and resources of its partner agencies – FBI, , Homeland Security Investigations (HSI), U.S. Customs and Border Protection (CBP), the Food and Drug Administration Office of Criminal Investigations (FDA-OCI), the U.S. Postal Inspection Service (USPIS), the U.S. Patent and Trademark Office (USPTO), INTERPOL, Mexican Revenue Service, Royal Canadian Mounted Police, Air Force Office of Special Investigations, Defense Criminal Investigative Service (DCIS), Naval Criminal Investigative Service (NCIS), U.S. Army Criminal Investigative Command Major Procurement Fraud Unit, Defense Logistics Agency Office of the Inspector General, Department of Commerce International Trade Administration, Consumer Product Safety Commission, National Aeronautics and Space Administration Office of the Inspector General, U.S. Department of State Office of Intellectual Property Enforcement and the General Services Administration Office of the Inspector General (GSA-OIG).

    - The IPR Center is a clearinghouse for complaints, referrals, and inquiries for IPR-related matters, including de-confliction of incoming case information. The IPR Center serves as the hub for the strategic planning of multi-jurisdictional case initiatives against the most significant threats to U.S. IP. As a key partner at the IPR Center, the FBI led or participated in numerous working groups and coordination meetings with key industry partners from the lengthy list of entities affected by IP crime.

    - The FBI provided funding, development, and hosting services for www.iprcenter.gov. This recently launched website serves as the central information portal for the IPR Center and its partners to inform the public, rights holders, victims, and other Government agencies about the threat from IPR violations and the IPR Center's efforts to combat it. The site contains, among other things, links to agency homepages, reference material, publications, press releases, and notices of upcoming events related to IPR.

- The FBI closely coordinated with the Intellectual Property Enforcement Coordinator (IPEC), Victoria Espinel and her staff. The FBI participated in working groups, briefings, joint strategic plan development, international capacity building/training initiatives, and provided FBI specific information for inclusion in the IPEC's bi-monthly newsletter. The FBI ensured its field IPR SAs were informed of the IPEC's mission, goals and strategy through communication with field offices and during training sessions.

    - The FBI actively participated and contributed to several U.S. Government working groups on IP enforcement and training, including the White House Anti-Counterfeiting Working Group and the Department of Justice's Joint Liaison Group (JLG) with China.

- FBI led the Intelligence Fusion Group (IFG) at the IPR Center with partner agencies to define the IPR threat picture/domain, share strategic intelligence, establish joint collection requirements, and produce joint intelligence products. In FY 2011 this effort was bolstered by the placement of two Intelligence Analysts (IAs) from the FBI's Intelligence Directorate into the FBI's IPRU at the IPR Center. These embedded IA's worked closely with IPRU investigative SAs and SSA program managers to identify emerging IP threats and trends and to produce a number of strategic and tactical intelligence reports.

    - As part of the IFG, the FBI collaborated and produced a joint IPR Center intelligence report entitled "Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad," publicly released in November 2011. This comprehensive study detailed various threats to United States IP from criminal violations and is intended to serve as a baseline assessment of the current IPR crime problem. Designed to provide valuable insight for law enforcement, industry, and public partners, the report was the culmination of a year-long effort to analyze Government and open source information, and document the input from over 100 domestic and international IPR experts in both industry and government.

The FBI recognizes the importance of liaison and engagement with rights holders, victim companies, and their representative organizations to better address the IPR threat and emerging trends, and to improve awareness of IP theft. In addition to routine and ongoing interaction related to specific cases and initiatives, the FBI participated in the following selected events in FY 2011:

- In February 2011, the FBI hosted a meeting of corporate security executives from key U.S. industries to examine trade secret and economic espionage risk and trends and to develop a working joint strategy to combat the problem.

- In February 2011, the FBI helped to organize, plan and develop the International Intellectual Property Crime Investigator's College (IIPCIC) in conjunction with INTERPOL. The IIPCIC is an online course designed to support international efforts to prevent, detect, investigate and prosecute transnational organized IP crime.

- In May 2011, the FBI participated in the Motor Equipment and Manufacturers Association (MEMA) Brand Protection Committee Spring Meeting to discuss current trends of IPR violations in the automotive industry and encourage future collaboration and case referrals.

- In May 2011, the FBI participated in roundtable discussions at the International Anti-Counterfeiting Coalition Conference.

- In June 2011, the FBI presented at Underwriters Laboratory IPR training for law enforcement on the FBI's IPR program and the efforts of the IPR Center. The training was attended by over 50 law enforcement officers including HSI, FBI, CBP, San Diego and Los Angeles Sherriff's offices.

- In June 2011, the FBI attended and presented at the Electronic Entertainment Expo's IPR training for law enforcement. The training focused on current trends and investigations involving online piracy of digital entertainment software.

- In June 2011, the FBI attended an industry based conference on counterfeit pharmaceuticals and received training for a number of investigative agents on this area of IPR violations.

- In July 2011, the FBI presented on the IPR program and the Fractured Skies initiative at the Aviation Supply Association (ASA) conference. The attendees included Fractured Skies partners from the FAA and targeted representatives from the aviation supply chain and manufacturing industry.

- In July 2011, the FBI attended the Department of Justice, Computer Crime and Intellectual Property Section's Annual IP Industry and Law Enforcement meeting. As part of this meeting, the FBI Assistant Director of its Cyber Division addressed industry leaders about the FBI's progress in IPR enforcement.

- The FBI provided IPR training to the Citizen's Academies from San Juan, PR; Knoxville, TN; Boston, MA; Kansas City, MO; New Orleans, LA and Birmingham, AL at FBIHQ regarding Cyber and IPR investigations. Citizen's Academies provide business, religious, community and civic leaders an inside look at the FBI and its mission.

- In July 2011, the FBI presented at the Coalition Against Counterfeiting and Piracy meeting at the U.S. Department of Commerce and discussed the FBI's progress

based upon the PRO-IP Act and the organization's role within the IPR Center.

- In August 2011, the FBI's New York office conducted dedicated IPR training for its agents and brought in brand protection and product security experts as keynote instructors.

- In September 2011, the FBI gave a presentation about trade secret risk and protections to security officials at a large defense contractor.

- In September 2011, the FBI participated in the 2011 IPR Center Symposium, "Online IP Theft in the 21st Century" which was attended by over 100 representatives from rights holders and their respective organizations. This was also attended by SAs from the field who received training and information on current trends and threats.

- At the FBI's request, the Department of Justice published a Notice of Proposed Rulemaking to make the FBI Anti-Piracy Warning Seal available to all copyright holders, subject to certain conditions. Currently, the Anti-Piracy Warning Seal is only available to members of five industry associations, including the Motion Picture Association of America, who have entered into written agreements with the FBI to use the warning. The public comment period for the proposed rule ended November 7, 2011, and the FBI is currently working toward publishing a Final Rule.

International Liaison and Training

During FY 2011, the FBI placed the first dedicated IPR SA at an overseas post. In September 2011, an IPR SA was deployed to the U.S. Embassy in Beijing, China for an initial tour of one year. This SA will work closely with his counterparts in Chinese law enforcement and with rights holders to advocate joint investigations and improve cooperation in this important region.

During FY 2011, the IPR Center hosted groups and delegations from numerous countries, including but not limited to, INTERPOL, EUROPOL, China, Australia, Mexico, Russia, Thailand, Vietnam and Paraguay. As a key partner at the IPR Center, the FBI participated in each of these visits and provided overviews of the FBI's role and structure with regard to IPR enforcement.

Through its international Legal Attache' network, the FBI also provided IPR presentations to international audiences in FY 2011, including the American Grey Market Association in Singapore in September 2010 and the opening of a new Underwriter's Laboratory in Copenhagen, also in September 2011.

The FBI recognizes the importance of providing useful, expert IPR training to our foreign counterparts. The FBI also recognizes the importance of fully supporting other USG

international training efforts. The following are selected international training efforts which were supported and/or led by the FBI in FY 2011:

- In October 2010, the FBI provided training and participated in INTERPOL's 2010 International Law Enforcement IP Crime Conference in Hong Kong, Special Administrative Region of the People's Republic of China, with more than 500 foreign law enforcement and industry representatives from 48 countries. The FBI presented on several topics, including combating online criminals in the 21st century and effective online anti-piracy teams to defeat cyber criminals.

- In March 2011, the FBI provided training and participated in a U.S. Patent and Trademark Office (USPTO) Enforcement workshop in Moscow, Russia focusing on copyright infringement in the digital environment.

- In March 2011, the FBI provided training as part of the USPTO Global Intellectual Property Academy (GIPA) and Association of Southeast Asian Nations (ASEAN) Workshop on IPR Enforcement on the Internet in Bangkok, Thailand. The FBI presented and participated in several panel discussions regarding criminal investigative techniques using the Internet and financial investigations in Internet piracy cases. In addition, the FBI has participated in GIPA training sessions for West African Nations and ASEAN nations in the United States.

- In May 2011, the FBI provided training during the Computer Forensics and Intellectual Property Crimes Conference in Mexico City, Mexico in May 2011. The conference was sponsored by the Department of Justice, FBI, and Mexico's Secretariat of Public Security and provided training regarding various crimes involving cyber technology; the search, preparation, and preservation of electronic evidence; and effectively utilizing international legal assistance during investigations. The FBI also provided subsequent training to federal judges from Mexico and the United States to educate them about the unique aspects of cyber and IP investigations.

- In June 2011, the FBI provided training at the USPTO Law Enforcement Workshop in Kyiv, Ukraine regarding IPR crime and investigations. The training, entitled "Copyright Infringement in the Digital Environment," focused on the collection of electronic evidence and conducting investigations in the online arena. Attendees included over 40 international government representatives, as well as 13 industry partners.

- As a member of the INTERPOL Intellectual Property Crime Action Group (IIPCAG), the FBI provided training and participated in the 2011 International Law Enforcement IP Crime Conference in Madrid, Spain. This conference is focused primarily on operational activities and brings together law enforcement organizations, regulatory agencies, private sector IP crime investigators and prosecutors to develop practical operational responses to IP crime. There were more than 400 foreign law enforcement and industry

representatives from close to 200 countries in attendance. The FBI benefits by attending and contributing to this conference. The FBI provides all translation services, making a targeted address to the conference as a whole, and leading several breakout sessions. This conference allows the FBI to: develop new relationships and enhance existing relationships with the law enforcement agencies of other countries responsible for responding to IPR issues; share trends and intelligence in regional and global IP crime; facilitate case referrals and lead generation and response; share best practices in IP enforcement efforts; and develop protocols for joint/cooperative responses to global IPR matters. Attendance by the FBI has directly resulted in investigative leads, case referrals, and international assistance in IPR investigations, and INTERPOL has recently moved to adopt a Theft of Trade Secrets program.

Looking Forward

At the close of FY 2011, the FBI has successfully built a robust and effective IP enforcement program that focuses on the most significant and serious threats to the U.S. economic and national security. Funds provided by the PRO-IP Act have provided direct support to innovative and significant IPR cases. The PRO-IP Act has provided 51 investigative agents to the field and personnel to the IPRU to address international and complex IPR matters. In addition, funding for training and outreach permitted the FBI to train dedicated IP agents in the nuances of IP enforcement and build bridges with rights holders in the private sector as well as internationally. Full integration and partnership at the National IPR Center has enabled the FBI to leverage these successes exponentially.

Looking forward, the FBI will strive to continue the strong momentum developed in FY 2011 through continuous and productive working relationships with its IPR Center partners, rights holders and groups, other USG agencies, and our foreign counterparts. The FBI will employ the resources provided by the PRO-IP Act to initiate, advance and support cutting edge and significant IPR investigations, initiatives, training, and projects. As a result of hard work and innovation, a number of significant and unprecedented investigations are anticipated to be completed in the upcoming year. Through its IPR representative in China, the FBI will seek to build closer working relationships with law enforcement professionals on the other side of the Pacific.

The threat to U.S. IP interests is immense and growing in size and scope, paralleling the sophistication of Internet based theft and computer network intrusions. IP crime is constantly evolving in complexity as are the challenges related to these investigations. The increase in global Internet penetration is accompanied with an increasingly international venue for IP crime, and the increased use of the Internet as a tool to facilitate IPR crime. The FBI recognizes these challenges and as in the past, will utilize its expertise and resources to lead the law enforcement response.