Department of Justice

STATEMENT OF

GORDON M. SNOW
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE

ENTITLED

"Oversight of Intellectual Property Law Enforcement Efforts**"**

PRESENTED

June 22, 2011

Good afternoon Chairman Leahy, Ranking Member Grassley, and members of the Committee. I'm pleased to appear before you today to discuss the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO IP Act) and the FBI's efforts, activities, and successes relating to intellectual property rights (IPR) crimes to date.

The enforcement of U.S. laws protecting IPR is critical to protecting the U.S. economy, our national security, and the health and safety of American citizens.

The increasing accessibility of the Internet and improvements in manufacturing and transportation have led to the expansion of the global market. With increasing competition, innovation, and divisions of labor, more digital content is instantaneously distributed to the global market than ever before. Businesses now have extraordinary opportunities to market and distribute their goods and services all around the world.

Unfortunately, the expansion in worldwide trade has led to growth in the number of criminals and organizations that seek to exploit and misappropriate the intellectual property of others for profit. These criminals have developed complex and diverse methods of committing IPR crime.

The Nature of the Threat

IPR violations which include theft of trade secrets, digital piracy, and the trafficking of counterfeit goods, result in billions of dollars in lost profits annually. Failure to protect IPR undermines confidence in the economy, removes opportunities for growth, erodes the U.S.'s technological advantage, and disrupts fairness and competitiveness in the marketplace. In short, a robust system for protecting IPR is critical to economic prosperity.

However, some IPR violations pose a more far-reaching and serious threat to the U.S. than just economic loss to the rights holder. Such violations put public safety at risk through the sale of counterfeit pharmaceuticals, electrical components, aircraft and automobile parts, and the funding of organized crime.

Some IPR violations also threaten our critical infrastructures and our national security. Counterfeit computer and networking devices undermine the reliability of our communications and transportation networks and create national security vulnerabilities. In addition, nation states target U.S. civilian industries for trade secret theft to obtain information that can be used to advance domestic industries and military capabilities.

The focus of my remarks today is the important role the FBI plays in protecting IPR, our efforts to coordinate with other federal agencies to ensure that intellectual property is rigorously protected, and our successes in this battle thus far.

The Role of the FBI

The FBI's strategic objective is to detect and disrupt state sponsored groups and international and domestic criminal organizations that manufacture counterfeit and pirated goods or steal, distribute or otherwise profit from the theft of intellectual property. The highest priorities for our investigations are counterfeit products affecting health and safety, the theft of trade secrets, and violations with a significant economic impact. The FBI aggressively pursues intellectual property enforcement through traditional investigative methods, intelligence initiatives and coordinated efforts with private industry and domestic and foreign law enforcement partners.

The FBI partners closely with the National Intellectual Property Rights Coordination Center (the IPR Center), which is hosted by U.S. Immigration and Customs Enforcement (ICE). The IPR Center serves as a centralized, multiagency entity to coordinate, manage, and advocate the U.S. government's criminal enforcement of intellectual property laws.

The FBI moved its Intellectual Property Rights Unit (IPRU) to the IPR Center in April 2010. It includes five dedicated FBI agents, as well as management staff, intelligence analysts and professional support staff who work full time at the IPR Center. The IPRU has a dual focused mission. First, it provides effective national program management for the FBI IPR program by aggressively advocating program awareness, coordinating and deconflicting investigative activity, and proactively developing relationships to address current and emerging threats to U.S. intellectual property. Second, it initiates and conducts IPR investigations that are complex, multi-jurisdictional and/or international in nature.

The IPRU is the coordination center for field office efforts to investigate IPR violations and other FBI divisions that conduct investigations with an IPR nexus. For example, the Criminal Investigative Division's Organized Crime Unit investigates cases involving counterfeit health products. The Counterintelligence Division's Economic Espionage Program focuses on the theft of trade secrets by foreign agents, governments and instrumentalities as defined by the Economic Espionage Act of 1996. Collaboration with these two divisions on IPR cases functions as a force multiplier and leads to broader criminal charges and higher penalties for offenders.

The FBI and the PRO IP Act

As a result of the PRO IP Act, the FBI Cyber Division has 51 dedicated IPR special agents placed in 21 field offices and the IPRU. The first enhancement under the Act, in April 2009, resulted in the allocation of 26 positions in the field and five at the IPRU. A second enhancement in May 2010 led to the allocation of an additional 20 positions in the field. Of these 51 positions, 44 special agents were placed in 20 field offices where United States Attorneys' Office (USAO) had Computer Hacking and Intellectual

Property (CHIP) Units. The FBI office in Houston was allocated two IPR agents, even thought there is not a CHIP unit there, for a total of 46 agents in the field.

As part of this allocation, the field offices in Los Angeles, New York, San Francisco, and Washington, D.C. received an enhancement to establish dedicated IPR squads. Each of these offices has established IPR task forces or working groups to coordinate IPR enforcement efforts and conduct outreach to industry and rights holders.

This distribution of investigative resources maximizes the nationwide reach and ability of the FBI to disrupt and dismantle international and domestic manufacturers or distributors of counterfeit and pirated goods, and criminal organizations engaged in IPR crime. The locations for the distribution of these resources were selected based on a regional domain analysis of the threat to intellectual property, intellectual property threat intelligence reporting, input from the IPR Center, and an understanding that the geographically-dispersed nature of IPR violations and subject locations made it possible to establish venues regionally. The placement of the special agents was coordinated with and approved by the Office of the Deputy Attorney General and the Executive Office of the United States Attorneys.

As of May 31, 2011, the FBI had 471 pending IPR investigations with 46 special agent positions dedicated to working IPR matters in the field. In FY 2010, the number of new FBI initiated theft of trade secrets and health and safety cases increased by 42 percent over FY 2009. The use of sophisticated investigative techniques increased by 50 percent in IPR cases.

In addition to the placement of IPR dedicated agent resources, in the spring of 2010, the IPRU management team conducted a case review of all pending IPR cases to support the shift of resources to priority investigations.

Strategic Initiatives and Successes

Capitalizing on the resources from the PRO IP Act, the FBI has enhanced its engagement on a number of significant strategic initiatives. This engagement has sharpened the focus of the FBI's IPR program on priority threats, increased awareness of the threat landscape, and strengthened relationships with community partners.

The FBI established and leads the Intelligence Fusion Group (IFG) at the IPR Center. Together the partner agencies define the IPR threat picture, share tactical and strategic intelligence, produce joint intelligence products, and develop the national strategy to address IPR crimes. Through the IFG, the FBI led a comprehensive analysis of the global threat to U.S. interests from criminal IPR violations. The report, entitled "Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad," is the culmination of a year-long joint effort led by the FBI and ICE with contributions from IPR Center partners. As part of this effort, agents and analysts interviewed 126 IPR experts from corporate security offices, industry associations, government agencies, and academic institutions in the U.S., India, and China regarding

IPR threats. A survey accompanying the report will solicit feedback and additional information to help determine additional targeted analysis opportunities.

To address the problem of counterfeit aircraft parts entering the commercial and military repair or manufacturing supply chain, the FBI, Department of Transportation Office of Inspector General and Federal Aviation Administration jointly coordinated the "Fractured Skies" initiative. As part of this effort, the IPRU has engaged the National Cyber-Forensics & Training Alliance, located in Pittsburgh, PA, for analytical review and target package development.

In an effort to improve international relationships on IPR investigations, conduct threat assessments, and make recommendations on the strategic plan in high threat countries, the IPRU embedded a dedicated IPR team comprised of an analyst and an agent in the FBI's Legal Attaché offices in Beijing and New Delhi to work directly with local and regional authorities on IPR matters for 60 days. Based upon the results of this effort and the threat emanating from these regions, the IPRU is currently in the process of embedding a fulltime IPR dedicated agent in Beijing for a year.

To capitalize on private sector partnerships, the FBI created a working group consisting of corporate security officers from Fortune 100 companies to focus on bolstering relationships of trust between law enforcement agencies and industry and improving information-sharing regarding intellectual property theft. In February 2011, the FBI hosted key industry Chief Security Officers to kick-off the Intellectual Property Threat Small Working Group. The goal of this working group is to build liaison among industry peers in an effort to generate high priority IPR cases. To this end, the FBI is currently developing targeted education and awareness presentations for corporate executives and general counsels.

Additionally, the FBI has taken over the hosting of the IPR Center's website, www.IPRCenter.gov. Phase two of this project will kick off later this year and involved a significant redesign of the site so that it includes training, education, enforcement activities and a reporting mechanism for IPR tips. The FBI is working in concert with the IPR Center partners to ensure comprehensive coverage of IPR issues and make this site the "go to" site for all IPR enforcement.

Training and Capacity Building

In order to promote high standards of IPR protection and the enforcement of laws protecting intellectual property, the FBI places a heavy emphasis on meaningful training and capacity building. The FBI provides training on IPR enforcement to an increasing number of individuals each year. In FY 2009, the FBI provided IPR training to 782 individuals from the federal government, the domestic private sector, foreign governments, and the overseas private sector. In FY 2010, the FBI trained 1678 such individuals. As of May 2011, the FBI has already trained 1064 individuals. As described below, the FBI provides training to its own personnel and its domestic and international

counterparts in a number of different ways. Resources from the PRO IP Act have made these ambitious and important training programs possible.

In September 2010 the IPRU provided its second annual, comprehensive IPR program training for IPR dedicated special agents. Additionally, special agents new to the IPR program received an introductory basic training course, and all IPR special agents participated in an advanced course to build upon existing skill sets and share the latest investigative techniques and technological methods.

IPR program coordinators in offices currently without funded IPR positions also received this annual training to ensure maximum regional coverage and to provide support to the CHIP units. The training session explored the forensic aspects of IPR investigations, to include the mechanisms necessary to identify counterfeits, the utilization of undercover operations, and IPR evidentiary procedures. Training topics also covered statutory authorities, DOJ enforcement efforts, major case initiatives, case studies, intelligence analysis for IPR cases, and federal partnering efforts. Industry subject matter experts from the International Anti-Counterfeiting Coalition, Underwriters Laboratories, Eli Lilly, Cisco Systems, the Motion Picture Association of America, and Microsoft made presentations.

All cyber career path designated special agents receive supplemental IPR training during a two-week New Agent Training (NAT) program. This training consists of an IPR program overview, a PRO IP Act overview, IPR case initiation/investigative techniques, and guidance regarding the importance of interagency partnerships, and the benefits of industry coordination efforts. The agents also receive forensic training from the Computer Analysis Response Team (CART) of the Operational Technology Division at FBI.

The IPRU recently developed a comprehensive web based training module specifically designed for agents working on IPR investigations. This module will be placed on our online training academy in the very near future.

The FBI also provides cross-program IPR training to organized crime and counterintelligence special agents and training on organized crime and counterintelligence to IPR dedicated special agents. This cross-program training was designed to ensure that agents pursue all avenues of investigation in cases that involve organized crime, counterintelligence and IPR issues.

The FBI provides IPR training to domestic and international law enforcement officials. The FBI is collaborating with its partner agencies to develop more comprehensive and advanced intellectual property training curriculum. The curriculum will ensure a uniform foundation across law enforcement agencies conducting IPR investigations and provide state and local law enforcement and industry liaisons with information about how to most effectively partner with the federal government on IPR investigations. For example, the FBI contributed training material and support to INTERPOL's new Intellectual Property

Crime College, an online resource available to law enforcement officers and industry partners worldwide.

Over the last two years, the FBI, through the IPRU, provided training on IPR to law enforcement officials from 15 different countries. For example, in September 2010, the FBI provided training during the 6th INTERPOL and Korea Copyright Commission Conference in Seoul, South Korea. It was the first to be held in the INTERPOL Asia and Pacific Region and was delivered with the support of the INTERPOL Liaison Office Bangkok for Asia and Pacific Region. The target audience included regional police middle managers with responsibility for investigating transnational organized intellectual property crime. The training provided attendees with a common understanding of the nature and extent of regional and increasingly global transnational organized intellectual property crime and investigative best practices techniques. It illustrated the benefits of working together with industries affected by intellectual property crime.

Additionally, the FBI provided training to the U.S. Patent and Trademark Office and its international attachés. The FBI's use of PRO IP Act resources has permitted an increased focus on training in high priority areas; this has directly contributed to increases in the quantity and quality of IPR cases.

Investigative Accomplishments

Pro IP Act resources have directly contributed to the FBI's development of strategic initiatives, training of its agents and counterparts, and increased capacity to combat high priority IPR crime. As a result, over the past year, the FBI and its partners have successfully investigated major IPR violations that resulted in millions of dollars in losses and unquantifiable harm to human health and safety. The following are but a few examples.

Earlier this year, a former Apple employee pled guilty to his role in a scheme to defraud Apple, Inc. while he was employed with the company from 2005 through 2010. The FBI investigation began in April 2010, when Apple found evidence of a kickback scheme on the employee's laptop. The employee transmitted Apple's confidential information, such as product forecasts, roadmaps, pricing targets, product specifications, and data obtained from Apple's business partners, to suppliers and manufacturers of Apple parts. In return, the suppliers and manufacturers paid kickbacks, including payments determined as a percentage of the business they did with Apple. The scheme enabled the suppliers and manufacturers to, among other things, negotiate more favorable contracts with Apple than they would have been able to obtain without the confidential information.

A joint investigation with an FBI counterintelligence squad revealed that General Motors (GM) was allegedly the victim of a conspiracy by a former GM employee and spouse to steal GM's hybrid vehicle technology with the intent to sell it to a Chinese automaker. The stolen GM documents were valued at over $40 million. The couple was arrested on July 22, 2010.

Last year, the FBI initiated a case involving the theft of trade secrets at Societe Generale (SocGen). On November 19, 2010, the former employee was found guilty of theft of trade secrets and interstate transportation of stolen property for stealing the proprietary computer code used in SocGen's high-frequency trading system; he was sentenced to three years in prison.

Similarly, a former employee of Goldman Sachs was convicted for theft of trade secrets in 2010. The defendant, a computer programmer, was accused of stealing trading software by uploading a proprietary trading platform program for equity products to a server in Germany. The FBI was able to seize the server in question and block access to the site. Goldman Sachs could not put an exact dollar amount on the software taken, but media reports have indicated that Goldman made in excess of $300 million in one year through its use of high frequency program trading and would not license the software for anything less than $1 billion. In December 2010, a federal jury found the defendant guilty of theft of trade secrets; in March 2011, he was sentenced to 97 months in prison.

Highlighting the potential for safety risks associated with some IPR violations, a Canadian man was sentenced to 33 months in prison for selling fake cancer medication on the Internet. Initial investigation into the sale and distribution of copyrighted media revealed that the subject was marketing fake cancer treatment drugs, which he admitted to selling to at least 65 cancer patients. In addition to his prison sentence, he was ordered to pay a $75,000 fine and $53,724 in restitution.

In January of this year, Wayne Chih-Wei Shu pled guilty to six counts of mail fraud, one count of trafficking in counterfeit goods, and one count of trafficking in counterfeit labels, illicit labels, or counterfeit documentation or packaging. The case was initially based on intelligence provided by Microsoft's Anti-piracy group which identified Shu as one of the most prolific distributors of counterfeit Microsoft server and Office software in Washington state. The investigation resulted in the seizure of the counterfeit evidence, as well as a forfeiture judgment for the sum of $1,750,396.98, for real and personal property, cash, and illicit proceeds.

Conclusion

As the Committee knows, law enforcement faces significant challenges in our efforts to protect IPR, thereby protecting U.S. IP right holders and the health and safety of American citizens.

With the support of the PRO IP Act, however, the FBI is in a position to aggressively investigate the domestic and international criminal organizations that profit from the theft of intellectual property. The PRO IP Act has enabled the FBI to dedicate increased numbers of special agents and analysts to IPR matters, ensure quality training, and support effective interagency collaboration. Combined with our ongoing efforts to strengthen our relationships with industry, partner with our counterparts in the IPR Center and improve our collaboration with our international law enforcement partners, these efforts will enhance our ability to identify and neutralize those who perpetrate IPR

crimes.

We look forward to working with the Committee and Congress as a whole to continue on a successful course forward for the nation that protects intellectual property and its citizens. Thank you for the opportunity to be here. I would be happy to take any questions.