THE

IP COMMISSION

THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY

The Commission on the Theft of American Intellectual Property is an independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academia, and politics.

IP COMMISSION 2019 REVIEW

Progress and Updated Recommendations

February 2019

Introduction

At the G-20 Summit in Buenos Aires in December 2018, President Trump and President Xi agreed to work toward a pathway for resolving trade disputes and announced a 90-day truce on raising tariffs. The two leaders stated they would "immediately begin negotiations on structural changes with respect to forced technology transfer, intellectual property (IP) protection, non-tariff barriers, cyber intrusions and cyber theft, services, and agriculture."

The IP Commission applauds the administration for seizing the unique opportunity afforded by increased attention on U.S.-China trade relations to address China's structural challenges that promote the theft of IP. This is the work of a generation, and the Commission urges our leaders to see it through.

While there have been many policy developments in the last 18 months related to strengthening the United States' ability to protect IP, there are still a number of ways we could improve those efforts. Below the IP Commission (1) highlights recent developments, (2) reviews new research that demonstrates the continued salience of IP protection to U.S. competitiveness, and (3) offers updated policy recommendations on page 4.

Recent Developments

IP raised to top-tier priority. The Trump Administration has elevated the elimination of China's theft of American IP, whether through cyber-theft, forced technology transfers, stolen trade secrets, counterfeiting of products, or other means, to one of the leading foreign policy priorities and a top goal of the U.S.-China economic negotiations.

Expanded Committee on Foreign Investment in the US (CFIUS) and export controls. The National Defense Authorization Act for Fiscal Year 2019 included the Foreign Investment Risk and Review Modernization Act (FIRRMA) to prevent acquisition of critical U.S. technologies through foreign investment and the Export Controls Act of 2018, which seeks to close loopholes in the export controls process by increasing restrictions on the transfer of emerging and foundational technologies to foreign persons. These new laws will significantly increase protection of IP, but more needs to be done.

Bill introduced to better combat threats to U.S. technology. Senators Rubio and Warner introduced a bipartisan bill in January of 2019 to establish an Office of Critical Technologies and Security to streamline efforts and ensure a whole-of-government approach to protecting U.S. technology. The IP Commission has argued that policy leadership for the protection of IP needs to be a responsibility of the National Security Advisor; this is a step in the right direction.

Increased oversight of military supply chains. The Pentagon has found a "surprising level of foreign dependence on competitor nations." While recent studies of the defense supply chain evaluate more than IP risks, they do include IP as a key factor in their assessments.

New Research

Over the last 18 months there has been a surge in research examining Chinese theft of U.S. IP that supports the IP Commission's findings:

The White House Office of Trade and Manufacturing Policy report on "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World" noted that Chinese economic espionage continues to increase and that China is the most active and persistent perpetrator of economic espionage. The report investigates the two primary forms of Chinese economic aggression: acquiring key technologies and IP from other countries, and capturing the emerging high-technology industries that will drive future economic growth and advancements in the defense industry. The report concludes that China engages in systematic economic espionage through a variety of means including cyber-espionage, evasion of export control laws, counterfeiting and piracy, reverse engineering, forced tech transfers, investment and licensing restrictions, data localization requirements, discriminatory IP protections, collection of science and technology information by Chinese nationals at universities, labs, and companies, and investments in private companies and university R&D programs.

The United States Trade Representative (USTR)'s "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974" examined China's industrial policies that call for the "absorption, digestion, and re-innovation of foreign intellectual property" to meet the Made in China 2025 goal of 40% self-sufficiency by 2020 and 70% by 2025. Many of China's means of acquiring IP are not officially written into law but are done in indirect and informal ways that make it difficult to prosecute. Through means such as investments and cyber intrusion, the Chinese government directs and unfairly facilitates the systematic acquisition of cutting-edge

U.S. technologies in industries deemed important by state industrial plans. The report concludes that China's acts, policies, and practices are unreasonable because they unfairly target critical U.S. technology with the goal of achieving dominance in strategic sectors. These practices harm U.S. innovation and economic competitiveness.

USTR's "2018 Report to Congress on China's WTO Compliance" found that despite repeated commitments to refrain from forcing U.S. companies to transfer technology, China continues to do so through market access restrictions, abuse of administrative processes, licensing regulations, asset purchases, and cyber and physical theft. Overall IP enforcement is hampered by gaps in rights protection, civil and administrative recourse mechanisms that fail to deter widespread IP infringement, and insufficient enforcement commitment. The resources, training, initiative, coordination, and transparency required to make real progress in IP enforcement remains lacking.

The Interagency Taskforce (led by Department of Defense) report on "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States" found that protection of the U.S. industrial base faces an unprecedented set of challenges, not least from the surprising level of dependence on suppliers in competitor nations. For instance, the report notes, "China is the single or sole supplier for a number of specialty chemicals used in munitions and missiles."

The U.S.-China Economic and Security Review Commission's "2018 Annual Report to Congress" noted the multiple challenges to protecting IP that U.S. firms face when operating in China. The report quotes the IP Commission's findings on the scale and scope of the problem and then delineates the policy tools that the United States has to respond to the theft of American IP. Of note, the Commission highlighted that Section 1637 of the 2015 National Defense Authorization Act gives the president authority—which has never been used—to "prohibit all transaction in property" of any person determined to have conducted "economic or industrial espionage in cyberspace."

The Department of Defense Defense Innovation Unit Experimental's report, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation" found that from 2015 to 2017, Chinese participation in venture-backed startups was at a record level of 10-16% of all venture deals (currently exceeds $100 billion), up from 6% from 2010 to 2015. China is especially investing in foundational technologies including artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics, gene editing, and blockchain technology. Investments in these technologies represented 40% of their investments in 2016. Many of these are dual-use technologies that will be key to the superiority of the U.S. military. As China seeks to meet its Made in China 2025 goals, it is ramping up its R&D spending to 2.5% of GDP and investing in mega projects in core electronics, chips, software, satellites, the next generation of broadband wireless communications, quantum communications, and classified defense projects. The Chinese Communist Party is highly involved in coordinating public and private investment and other vehicles of technology transfer to accomplish its economic and strategic goals. The report recommends the United States implement defensive policies such as CFIUS and export controls reforms (already in progress), introduce immigration and visa policy reforms for foreign students so they can stay in the United States with the knowledge they have attained at U.S. graduate schools, and increase the level of counterintelligence resources. Recommended proactive policies include increased funding for research, incentives for U.S. students to study STEM fields, pro-growth and productivity-enhancing economic policies, and finally, a whole-of-government approach with a coordinated strategy across multiple agencies and departments.

USTR's 2018 Special 301 Report placed China on the Priority Watch List due to critical IP concerns, including trade secret theft, online piracy and counterfeiting, a high volume of manufacturing and exporting counterfeit goods, technology transfer requirements, mandatory application of adverse terms to foreign IP licensors, localization requirements, and weak enforcement. The report points out that China has continuously failed to implement its promises to strengthen IP protection. However, there is positive momentum in China's judicial reforms that include its specialized IP courts and tribunals, which demonstrate competence, expertise, and transparency to a greater degree than other Chinese courts. Notwithstanding these positive developments, interventions by local government officials, powerful local interests, and the Chinese Communist Party remain obstacles to the independence of the courts and rule of law.

MITRE's "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War" report made a sophisticated argument for the importance of understanding supply chain security of the defense industrial base—of which the protection of IP is a critical element—as a fundamental component of national security in an era and environment of changing and increasingly asymmetric threat.

What Remains: IP Commission Updated Recommendations

There has been much progress in research and legislative and administrative action, but there are a number of ways the United States could be more effective in addressing IP theft. Some of these approaches include:

Build independent international database for scoring of entities from foreign countries that pose IP risk

Given the vast number of foreign actors and products in the U.S. marketplace and supply chains that present IP risks, no bureaucratic mechanism can cover the breadth of the problem and effectively prevent the theft of IP. For this reason, the IP Commission proposes to develop a market-based "scoring" system to rate foreign entities from countries known to pose IP risks that seek to do business with U.S. companies or government agencies. Such an approach would incentivize all actors to comply with international laws and values of liberal market economies, as the market would reward entities that score highly with more business and investment opportunities.

The score would draw upon globally sourced, existing data and must be objective and not subject to manipulation. A trusted score of this type, similar to a FICO credit score, will empower all law-abiding companies, organizations, government agencies, and individuals to make more educated decisions about the level of risk they are incurring before doing business with a foreign entity.

There is currently no mechanism that helps U.S. businesses understand the level of risk they face when engaging with a foreign company or that helps the U.S. government identify which companies should not be allowed to invest or do business in the United States. While the Bureau of Industry and Security in the Department of Commerce maintains a denied persons and entity list, this is solely for export controls. Export controls are not effective in preventing the loss of IP. For example, even at the height of the Cold War in the context of a much simpler global economy, the Soviet Union successfully evaded U.S. export controls. The updated CFIUS law, while an improvement, focuses on investment and thus misses the variety of other ways that bad actors siphon off IP.

The recommended database should begin with scoring Chinese actors (including companies and their subsidiaries, state-owned enterprises, and individuals) and then could expand to other countries that pose a national security challenge. The information in this database should be developed in coordination with U.S. allies to enable swift and harmonized responses. Adoption of the scoring system must cause the least possible disruption to the normal course of business.

Use the emergency economic powers already granted to the president to deny access to the U.S. market and banking system to foreign entities found to be directly benefitting from the theft of American IP

Under the International Emergency Economic Powers Act of 1977, the president is allowed to sanction individuals and organizations and to "prohibit any transaction in foreign exchange." Section 1637 of the 2015 National Defense Authorization Act expands this authority to cover "all transactions in property" of any person the president determines "knowingly engages in economic or industrial espionage in cyberspace." We need to make sure the president is using all of these tools that are at his disposal.

Deny access to banking system to foreign entities that use or benefit from the theft of American IP

No foreign entity that steals IP should be able to access the U.S. banking system. The secretary of the treasury should have the authority to deny access to the U.S. banking system to malicious actors. This builds on the existing statutory authority of the president as outlined above and was proposed but not adopted during the prior administration. The IP Commission strongly encourages the adoption of this recommendation to ensure that the United States is well placed to address new and emerging threats on an ongoing basis.

Enforce strict supply-chain accountability for the U.S. government

The IP Commission applauds the Pentagon's announcement that it will audit the U.S. military supply chain to identify weaknesses in the nation's military readiness, as well as former Secretary Mattis's announcement of the Protecting Critical Technology Task Force (PCTTF) to spot leaks in the military supply chain. The Commission recommends increased oversight of supply chains be expanded to the entire U.S. government.

Require the Securities and Exchange Commission to judge whether companies' use of stolen IP is a material condition that ought to be publicly reported

This recommendation is derived from strengthened accountability requirements on foreign firms that seek to be listed on U.S. exchanges. It was included in the original IP Commission report and merits further study.

Instruct the Federal Trade Commission to obtain meaningful sanctions against foreign companies using stolen IP

This recommendation seeks to find meaningful ways to punish willful IP-thieving entities. The modalities of how to do this in effective ways also merit deeper research and policy analysis.

Coordinate investment and export controls

The reforms passed on the CFIUS and the export controls processes in the recent National Defense Authorization Act made enormous strides forward by restricting investment in and potential exports of emerging technologies critical for national security. Now it is urgent that both the Department of the Treasury (which manages CFIUS) and the Department of Commerce (which manages export controls) work closely together to close loopholes and share information on foreign actors that pose risks.

Quickly intercept counterfeit goods

More must be done to quickly identify and intercept counterfeit goods coming into our ports. Development and deployment of new technologies to improve the ability to detect counterfeit goods can support law enforcement in this process. The Commission also recommends strengthening the International Trade Commission's 337 process to sequester goods containing stolen IP.

Streamline the process for reporting and responding to IP theft

The process to stop the sale of products made with stolen IP, especially stolen trade secrets, is costly and time-consuming, and by the time law enforcement and the courts take action the innovator's entire business might have been decimated. For example, by the time that the U.S. Department of Commerce in September 2018 took action against the imports of unfairly subsidized quartz countertops made with stolen technology, Chinese imports were supplanting $1.2 billion of sales per year of U.S.-produced quartz countertops for the American market. There needs to be a simpler way for businesses to report cases of IP theft, for law enforcement to take swift action to bar the sale of the illicit product, and for investigations to quickly proceed and come to conclusion. Authorities must act with haste—within hours or days, not weeks or months.

Establish multilateral policy dialogues

The Commission recommends the United States initiate multilateral policy dialogues with like-minded partners to strengthen and coordinate national policies on Chinese foreign investment and enforcement of IP laws, share information on foreign actors engaging in IP theft, and learn from each other's best practices. The Commission recommends starting with Japan, then including the European Union (especially Germany and France), Australia, and perhaps the Republic of Korea, Taiwan, and Singapore.

Utilize multilateral institutions to harmonize national and international legal and regulatory frameworks

While multilateral institutions like the World Trade Organization (WTO) and World Intellectual Property Organization (WIPO) are not always the most efficient and effective at providing protection of IP from an infringer like China, they can provide an important forum for allies committed to the rule of law and fair markets to chart a path forward, and to incentivize others to adopt the requisite norms and practices. The Commission applauds the United States, Japan, and the EU for their conversations on the sidelines of the WTO on forced technology transfers in China, Chinese industrial subsidies, and reforms to the WTO to better deal with IP violations. The Commission encourages these side dialogues to continue, and recommends bringing in other champions of free trade and high standards for IP protection.

ABOUT THE IP COMMISSION

The IP Commission is an independent and bipartisan initiative of American leaders from the private sector, public service in national security and foreign affairs, academia, and politics. The IP Commission published **reports** in 2013 and 2017 documenting and assessing the causes, scale, and other major dimensions of international intellectual property theft as they affect the United States. The reports also proposed appropriate U.S. policy responses that would mitigate ongoing and future damage of intellectual property rights by China and other infringers.

ABOUT THE COMMISSIONERS

Co-chairs:

- Admiral Dennis C. Blair, Co-chair of the IP Commission; Chairman of the board and Distinguished Senior Fellow at the Sasakawa Peace Foundation USA; former commander of the U.S. Pacific Command; and former U.S. director of national intelligence
- Craig Barrett, former chairman and CEO of Intel Corporation

Other Commissioners:

- Charles W. Boustany Jr., former six-term U.S. representative from Louisiana
- Slade Gorton, former U.S. senator from Washington State; member of the 9/11 Commission
- William J. Lynn III, CEO of Leonardo North America and DRS Technologies
- Deborah Wince-Smith, President and CEO of the Council on Competitiveness
- Michael K. Young, President of Texas A&M University