Information about the Department of Justice’s China Initiative and a compilation of China related criminal cases since Jan. 2018

Background

The People’s Republic of China is implicated in more than 80-percent of all economic espionage charges brought by the U.S. Department of Justice (DOJ) since 2012 and there is a nexus to China in more than 60-percent of all trade secret theft cases that the DOJ has charged.

The Department of Justice’s China Initiative reflects the strategic priority of countering Chinese national security threats and reinforces the President’s overall national security strategy. The Initiative was launched against the background of previous findings by the Administration concerning China’s practices. In March 2018, the Office of the U.S. Trade Representative announced the results of an investigation of China’s trade practices under Section 301 of the Trade Act of 1974. It concluded, among other things, that a combination of China’s practices are unreasonable, including its outbound investment policies and sponsorship of unauthorized computer intrusions, and that “[a] range of tools may be appropriate to address these serious matters.”

In June 2018, the White House Office of Trade and Manufacturing Policy issued a report on “How China’s Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World,” documenting “the two major strategies and various acts, policies, and practices Chinese industrial policy uses in seeking to acquire the intellectual property and technologies of the world and to capture the emerging high-technology industries that will drive future economic growth.”

In addition to identifying and prosecuting those engaged in trade secret theft, hacking and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats including foreign direct investment, supply chain threats and the foreign agents seeking to influence the American public and policymakers without proper registration.

The China Initiative falls under the Department’s National Security Division (NSD), which is responsible for countering nation-state threats to the country’s critical infrastructure and private sector.

China Initiative Leadership

- John C. Demers is the Assistant Attorney General for National Security and leads the China Initiative

U.S. Attorneys in the China Initiative Working Group

- Andrew E. Lelling (District of Massachusetts)
- Jay E. Town (Northern District of Alabama)
- Alex G. Tse (Northern District of California)
- Richard P. Donoghue (Eastern District of New York)
- Erin Nealy Cox (Northern District of Texas)

Components of Initiative

- The Attorney General has set the following goals for the Initiative:
  - Identify priority trade secret theft cases, ensure that investigations are adequately resourced; and work to bring them to fruition in a timely manner and according to the facts and applicable law;
  - Develop an enforcement strategy concerning non-traditional collectors (e.g., researchers in labs, universities, and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests;
  - Educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus;
  - Apply the Foreign Agents Registration Act to unregistered agents seeking to advance China’s political agenda, bringing enforcement actions when appropriate;
• 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;
• Implement the Foreign Investment Risk Review Modernization Act (FIRMA) for DOJ (including by working with Treasury to develop regulations under the statute and prepare for increased workflow);
• Identify opportunities to better address supply chain threats, especially ones impacting the telecommunications sector, prior to the transition to 5G networks;
• Identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses;
• Increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States; and
• Evaluate whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.

China-Related Cases since January 2018: Summarized

Friday, November 22, 2019

Former CIA Officer Sentenced for Conspiracy to Commit Espionage

A former Central Intelligence Agency (CIA) case officer was sentenced today to 19 years in prison for conspiring to communicate, deliver and transmit national defense information to the People’s Republic of China (PRC).

Thursday, November 21, 2019

Chinese National Who Worked at Monsanto Indicted on Economic Espionage Charges

Haitao Xiang, 42, formerly of Chesterfield, Missouri, was indicted today 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.

Thursday, November 14, 2019

Two Former Executives of the China Subsidiary of a Multi-Level Marketing Company Charged for Scheme to Pay Foreign Bribes and Circumvent Internal Accounting Controls

Summary: The former head of the China subsidiary of a publicly traded international multi-level marketing company (Company-1) and the former head of the external affairs department of the China subsidiary of the same company were charged today for their roles in a scheme to violate the anti-bribery and the internal control provisions of the Foreign Corrupt Practices Act (FCPA).

Tuesday, November 12, 2019

Chinese National Pleads Guilty to Committing Theft of Trade Secrets

Summary: Hongjin Tan, a 35 year old Chinese national and U.S. legal permanent resident, pleaded guilty Tuesday in federal court to committing theft of trade secrets from his employer, a U.S. petroleum company.

Friday, November 1, 2019

U.S. Navy Officer, His Wife, and Two Chinese Nationals Charged with Conspiring to Smuggle Military Style Inflatable Boats and Evinrude Military Outboard Motors to China

Summary: Assistant Attorney General John C. Demers and U.S. Attorney Maria Chapa Lopez for the Middle District of Florida announced the return of an indictment of four individuals, including two Chinese nationals, an active-duty United States Navy officer, and his wife, on charges relating to a conspiracy to unlawfully smuggle military-style inflatable boats, with Evinrude MFE military outboard motors, to the People’s Republic of China. The Navy officer and two other defendants have also been
charged with conspiring to violate firearms law, and the Navy officer has been charged with an
additional firearms-related offense and with making false official statements.

Friday, October 18, 2019

**Chinese National Sentenced to 40 Months in Prison for Conspiring to Illegally Export Military-and Space-Grade Technology from the United States to China**

Summary: On October 16, 2019, United States District Judge Diane J. Humetewa sentenced Tao Li, a 39-year-old Chinese national, to 40 months in prison, followed by three years of supervised release. Li had previously pleaded guilty to conspiring to export military and space-grade technology to the People’s Republic of China without a license in violation of the International Emergency Economic Powers Act.

Tuesday, September 24, 2019

**Former Intelligence Officer Convicted of Attempted Espionage Sentenced to 10 Years in Federal Prison**

Summary: Ron Rockwell Hansen, 60, of Syracuse, Utah, a former Defense Intelligence Agency (DIA) officer, who pleaded guilty in March to attempting to communicate, deliver, or transmit information involving the national defense of the United States to the People’s Republic of China, will serve 10 years in federal prison.

Monday, September 30, 2019

**Northern California Resident Charged with Acting as an Illegal Agent**

Summary: Xuehua Peng, also known as Edward Peng, was charged for acting as an illegal foreign agent in delivering classified United States national security information to officials of the People’s Republic of China’s Ministry of State Security (MSS).

Monday, September 16, 2019

**Chinese Government Employee Charged in Manhattan Federal Court with Participating in Conspiracy to Fraudulently Obtain U.S. Visas**

Summary: Zhongsan Liu was arrested and was charged by complaint for his involvement in a conspiracy to fraudulently obtain U.S. visas for Chinese government employees.

Monday, September 16, 2019

**Couple Who Worked at Local Research Institute for 10 Years Charged with Stealing Trade Secrets, Wire Fraud**

Summary: A former Dublin, Ohio, couple has been charged with crimes related to stealing exosome-related trade secrets concerning the research, identification and treatment of a range of pediatric medical conditions.

Wednesday, August 21, 2019

**University of Kansas Researcher Indicted for Fraud for Failing to Disclose Conflict of Interest with Chinese University**

Summary: Feng “Franklin” Tao, an associate professor at Kansas University was indicted on federal charges for hiding the fact he was a full-time employee for Fuzhou University, a Chinese university, while doing research at KU funded by the U.S. government. He was charged with one count of wire fraud and three counts of program fraud.

Tuesday, July 23, 2019
Four Chinese Nationals and Chinese Company Indicted for Conspiracy to Defraud the United States and Evade Sanctions

Summary: A federal grand jury charged four Chinese nationals and a Chinese company with violating the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA and defraud the U.S.; conspiracy to violate, evade and avoid restrictions imposed under the Weapons of Mass Destruction Proliferators Sanctions Regulations; and conspiracy to launder monetary instruments. The company are alleged to have tried to obscure illicit financial dealings on behalf of sanctioned North Korean entities that were involved in the proliferation of weapons of mass destruction.

Thursday July 11, 2019

Newly Unsealed Federal Indictment Charges Software Engineer with Taking Stolen Trade Secrets to China

Summary: Xudong Yao, also known as “William Yao,” a software engineer at a suburban Chicago locomotive manufacturer was charged with nine counts of theft of trade secrets for allegedly stealing proprietary information from the company and taking them to China.

Tuesday, July 9, 2019

Former State Department Employee Sentenced for Conspiring with Chinese Agents

Received Tens of Thousands of Dollars in Benefits from Two Chinese Agents in Exchange for Internal State Department Documents

Summary: Candace Marie Clairborne, a former employee of the U.S. Department of State, was sentenced to 40 months in prison, three years of supervised release and a fine of $40,000. Clairborne was found guilty of conspiracy to defraud the United States by lying to law enforcement and background investigators, and hiding her extensive contacts with, and gifts from, agents of the People’s Republic of China in exchange for providing them with internal documents form the U.S. State Department.

Tuesday, July 2, 2019

Electrical Engineer Convicted of Conspiring to Illegally Export to China Semiconductor Chips with Missile Guidance Applications

Summary: Yi-Chi Shih, an electrical engineer, was found guilty of multiple criminal charges, including a scheme to illegally obtain integrated circuits with military applications that later were exported to China without the required export license. After a six-week trial, Shih was found guilty of conspiracy to violate the International Emergency Economic Powers Act, a federal law that makes certain unauthorized exports, among other things, illegal.

Friday, May 17, 2019

Former CIA Officer Sentenced to Prison for Espionage

Summary: Former U.S. Intelligence officer Kevin Patrick Mallory was convicted under the Espionage Act for conspiracy to transmit national defense information to an agent of the People’s Republic of China. He was sentenced to 20 years in prison followed my five years of supervised release.

Wednesday, May 1, 2019

Former CIA Officer Pleads Guilty to Conspiracy to Commit Espionage
Summary: A former Central Intelligence Agency case officer pleaded guilty to conspiring to communicate, deliver and transmit national defense information to the People’s Republic of China. The officer, Jerry Chun Shing Lee, left the CIA in 2007 and moved to Hong Kong, where he accepted hundreds of thousands of dollars in cash in exchange sensitive information about the CIA, including national defense information.

**Wednesday, April 24, 2019**

**Former State Department Employee Pleads Guilty to Conspiring with Foreign Agents**

**Defendant Admitted Receiving Tens of Thousands of Dollars in Benefits From Two Chinese Agents in Exchange for Internal State Department Documents**

Summary: Candace Marie Claiborne, a former employee of the U.S. Department of State, pleading guilty today to a charge of conspiracy to defraud the United States, by lying to law enforcement and background investigators, and hiding her extensive contacts with, and gifts from, agents of the People’s Republic of China (PRC), in exchange for providing them with internal documents from the U.S. State Department.

**Tuesday, April 23, 2019**

**Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE’s Trade Secrets**

Summary: An indictment unsealed April 23 charged Xiaqing Zheng and Zhaoxi Zhang with economic espionage and conspiring to steal General Electric’s (GE’s) trade secrets surrounding turbine technologies, knowing and intending that those stolen trade secrets would be used to benefit the People’s Republic of China. The 14-count indictment alleged Zheng, while employed at GE Power & Water exploited his access to GE’s files by stealing multiple electronic files and emailing and transferring them to Zhang, his business partner in China.

**Wednesday, April 17, 2019**

**Former Manager for International Airline Pleads Guilty to Acting as an Agent of the Chinese Government**

**Defendant Placed Packages on Flights from JFK Airport to Beijing at the Direction of Military Officers Assigned to the Chinese Mission to the United Nations**

Summary: Ying Lin, a former manager with an international air carrier headquartered in the People’s Republic of China (PRC), pleaded guilty to acting as an agent of the PRC, without notification to the Attorney general, by working at the direction and control of military officers assigned to the Permanent Mission of the People’s Republic of China to the United Nations. Lin abused her privileges to transport packages from John F. Kennedy International Airport to the PRC at the orders of the Chinese military officers and in violation of Transportation Security Administration regulations.

**Friday, March 15, 2019**

**Former Defense Intelligence Officer Pleads Guilty to Attempted Espionage**

Summary: Ron Rockwell Hansen, a former Defense Intelligence Agency officer pleaded guilty in connection with his attempted transmission of national defense information to the People’s Republic of China. Hansen’s sentencing is scheduled for Sept. 24, 2019. Hansen is a retired U.S. Army Warrant Officer with background in signals intelligence and human intelligence. He was hired by the DIA as a civilian intelligence case officer in 2006, where he held Top Secret clearance for many years, and signed several non-disclosure agreements during his tenure at DIA and as a government contractor. Hansen received hundreds of thousands of dollars in compensation for providing information to agents of the Chinese intelligence service.

**Friday, February 15, 2019**
Chinese National Sentenced to Prison for Selling Counterfeit Computer Parts

Summary: Ruiyang Li, a man from Beijing, China, was sentenced to serve 54 months in federal prison for directing the shipment of counterfeit computer-networking equipment into the Southern District of Texas. Since Li is not a U.S. citizen, he is expected to be deported after serving his prison sentence.

Thursday, February 14, 2019

One American and One Chinese National Indicted in Tennessee for Conspiracy to Commit Theft of Trade Secrets and Wire Fraud

Summary: A grand jury sitting in Greeneville, Tennessee has returned an indictment against Xiaorong You, also known as Shannon You, and Liu Xiangchen, 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 indictment alleges that You, Liu, and a third co-conspirator planned for You to exploit her employment with American employers to steal trade secrets and provide the information for the economic benefit of trade secrets the Chinese company that Liu managed. Liu’s company planned to manufacture and profit form the products developed using the stolen trade secrets. In exchange, Liu and her company would financially reward You.

Monday, January 28, 2019

Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice

Huawei Corporate Entities Conspired to Steal Trade Secret Technology and Offered Bonus to Workers who Stole Confidential Information from Companies Around the World

Summary: A 10-count indictment unsealed in the Western District of Washington State charged Huawei Device Co., Ltd. and Huawei Device Co. USA with theft of trade secrets conspiracy, attempted theft of trade secrets, seven counts of wire fraud, and one count of obstruction of justice. The indictment, returned by a grand jury on January 16, details Huawei’s efforts to steal trade secrets from T-Mobile USA and then obstruct justice when T-Mobile threatened to sue Huawei in U.S. District Court in Seattle. The alleged conduct described in the indictment occurred from 2012 to 2014, and includes an internal Huawei announcement that the company was offering bonuses to employees who succeeded in stealing confidential information from other companies.

Monday, January 28, 2019

Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud

Huawei Device USA Inc. and Huawei’s Iranian Subsidiary Skycom Also Named Defendants Other Charges Include Money Laundering, Conspiracy to Defraud the United States, Obstruction of Justice and Sanctions Violations

Summary: A 13-count indictment unsealed in a federal court in Brooklyn, New York, charged four defendants — Huawei Technologies Co. Ltd., Huawei Device USA Inc., Skycom Tech Co. Ltd., and Huawei’s Chief Financial Officer Wanzhou Meng — with various crimes. Huawei and Skycom are charged with bank fraud, and conspiracy to commit bank fraud, wire fraud and conspiracy to commit wire fraud, violations of the International Emergency Economic Powers Act (IEEPA) and conspiracy to violate IEEPA, and conspiracy to commit money laundering. Huawei and Huawei USA are charged with conspiracy to obstruct justice related to the grand jury investigation in the Eastern district of New York. Meng is charged with bank fraud, wire fraud, and conspiracies to commit bank and wire fraud.

Friday, December 21, 2018

Chinese National Charged with Committing Theft of Trade Secrets
Summary: Hongjin Tan, a 35 year old Chinese national and U.S. legal resident was arrested and charged with theft of trade secrets and is alleged to have stolen the trade secrets from his employer, a U.S. petroleum company.

**Wednesday, December 5, 2018**

**Former Head of Organization Backed by Chinese Energy Conglomerate Convicted of International Bribery, Money Laundering Offenses**

Schemed to Bribe the President of Chad, President and Foreign Minister of Uganda

Summary: Chi Ping Patrick Ho, the head of the China Energy Fund Committee, a nongovernmental organization, was convicted on seven counts for his participation in a multi-year, multimillion-dollar scheme to bribe top officials of Chad and Uganda in exchange for business advantages for a Chinese oil and gas company. After a one-week jury trial, HO was found guilty of one count of conspiring to violate the Foreign Corrupt Practices Act (FCPA), four counts of violating the FCPA, on count of conspiring to commit international money launder and one count of committing international money laundering.

**Thursday, November 1, 2018**

**PRC State-Owned Company, Taiwan Company, and Three Individuals Charged With Economic Espionage**

Summary: A federal grand jury indicted a state-owned enterprise of the People’s Republic of China (PRC), a Taiwan company, and three individuals, charging them with crimes related to a conspiracy to steal, convey, and possess stolen trade secrets of an American semiconductor company for the benefit of a company controlled by the PRC government. All of the defendants are charged with a conspiracy to commit economic espionage, among other crimes. In addition, the United States filed a civil lawsuit seeking to enjoin the further transfer of the stolen trade secrets and to enjoin certain defendants from exporting to the United States any products manufactured by UMC or Jinhua that were created using the trade secrets at issue.

**Tuesday, October 30 2018**

**Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years**

Summary: Chinese intelligence officers and those working under their direction, which included hackers and co-opted company insiders, conducted or otherwise enabled repeated intrusions into private companies’ computer systems in the United States and abroad for over five years. The conspirators’ ultimate goal was to steal, among other data, intellectual property and confidential business information, including information related to a turbofan engine used in commercial airliners.

**Wednesday, October 10, 2018**

**Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies**

Summary: A Chinese Ministry of State Security (MSS) operative, Yanjun Xu, aka Qu Hui, aka Zhang Hui, was arrested and charged with conspiring and attempting to commit economic espionage and steal trade secrets from multiple U.S. aviation and aerospace companies. Xu was extradited to the United States on Oct. 9, 2018. Xu is a Deputy Division Director with the MSS’s Jiangsu State Security Department, Sixth Bureau. The MSS is the intelligence and security agency for China and is responsible for counter-intelligence, foreign intelligence and political security. MSS has broad powers in China to conduct espionage both domestically and abroad. He was charged with conspiring and attempting to commit economic espionage and theft of trade secrets.

**Tuesday, September 25, 2018**
Chinese National Arrested for Allegedly Acting Within the United States as an Illegal Agent of the People’s Republic of China

Summary: Ji Chaoqun, a Chinese citizen residing in Chicago, was arrested for allegedly acting within the United States as an illegal agent of the People’s Republic of China. Ji was charged with one count of knowingly acting in the United States as an agent of a foreign government without prior notification to the Attorney General. He was tasked with providing a high-level intelligence officer in the Jiangsu Province Ministry of State Security with biographical information on eight individuals for possible recruitment by the JSSD.

Friday, June 8, 2018

Jury Convicts Former CIA Officer of Espionage

Summary: A federal jury convicted Kevin Patrick Mallory, a former Central Intelligence Agency case officer on espionage charges related to his transmission of classified documents to an agent of the People’s Republic of China. Mallory has held numerous positions with various government agencies and several defense contractors, including working as a covert case officer for the CIA and an intelligence officer for the Defense Intelligence Agency. Because of his various government positions, Mallory obtained a Top Secret security clearance. He was convicted of conspiracy to deliver, attempted delivery, delivery of defense information to aid a foreign government, and making material false statements.

Friday, April 27, 2018

Two Businessmen Charged With Conspiring to Commit Economic Espionage for Benefit of Chinese Manufacturing Company

Case Involves Dual-Use Technology with Military Applications

Summary: Two business men, including one who is a Chinese national, were indicted on charges alleging they conspired to commit economic espionage and steal trade secrets from a business in the United States on behalf of a company in China that was engaged in manufacturing buoyancy materials for military and civilian uses.

Wednesday, April 4, 2018

Chinese Scientist Sentenced to Prison in Theft of Engineered Rice

Summary: Chinese scientist Weiqiang Zhang, a Chinese national, and U.S. legal permanent resident, was sentenced to 121 months in a federal prison for conspiring to steal samples of a variety of rice seeds from a Kansas biopharmaceutical research facility. Zhang acquired without authorization hundreds of rice seeds produced by his employer, Ventria Bioscience, hundreds of rice seeds. The seeds were found by U.S. Customs and Border Protection officers in the luggage of Zhang’s visitors as they prepared to leave the U.S. for China.

Friday, January 19, 2018

2 Los Angeles-Area Men Charged with Conspiring to Illegally Obtain Technology and Computer Chips that Were Sent to China

Summary: Federal authorities arrested Yi-Chi Shih and Kiet Ahn Mai on charges of conspiracy. Shih is also charged with violating the International Emergency Economic Powers Act (IEEPA), which makes certain unauthorized exports illegal. A criminal complaint alleges that Shih and Mai conspired to illegally provide Shih with unauthorized access to a protected computer of a United States company that manufactured specialized, high-speed computer chips known as monolithic microwave integrated circuits (MMICs). The conspiracy count also alleges that the two men engaged in mail fraud, wire fraud and international money laundering to further the scheme.

Thursday, January 18, 2018
Chinese National Sentenced for Economic Espionage and Theft of a Trade Secret from U.S. Company

Summary: Xu Jiaquiang, a Chinese national, was sentenced to five years in prison, for economic espionage and theft of a trade secret in connection with Xu’s theft of proprietary source code from Xu’s former employer, with intent to benefit the National Health and Family Planning Commission of the People’s Republic of China.