Information about the Department of Justice's Attorney General China Initiative, AAG Demers bio and a compilation of China related criminal cases since Jan. 2018

Attorney General China Initiative Fact Sheet

Background

The Attorney General's Initiative reflects the Department's strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy. The Initiative is 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 a months' long 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."

The National Security Division (NSD) is responsible for countering nation state threats to the country's critical infrastructure and private sector. 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.

Statements

Assistant Attorney for National Security John C. Demers

"China wants the fruits of America's brainpower to harvest the seeds of its planned economic dominance. Preventing this from happening will take all of us, here at the Justice Department, across the U.S. government, and within the private sector. With the Attorney General's initiative, we will confront China's malign behaviors and encourage them to conduct themselves as they aspire to be: one of the world's leading nations."

FBI Director Christopher Wray

"No country presents a broader, more severe threat to our ideas, our innovation, and our economic security than China," said FBI Director Christopher Wray. "The Chinese government is determined to acquire American technology, and they're willing use a variety of means to do that – from foreign investments, corporate acquisitions, and cyber intrusions to obtaining the services of current or former company employees to get inside information. If China acquires an American company's most important technology – the very technology that makes it the leader in a field – that company will suffer severe losses, and our national security could even be impacted. We are committed to continuing to work closely with our federal, state, local, and private sector partners to counter this threat from China."

US Attorneys in 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.

The Honorable John Demers Leads the DOJ China Initiative

John Demers became Assistant Attorney General for National Security on February 22, 2018. In that capacity, he leads the Department of Justice's efforts to combat national security related cyber-crime, terrorism and espionage, to enforce export control and sanctions laws, to use the authorities of the Foreign Intelligence Surveillance Act, and to conduct national security review of foreign investments. In November 2018, John was selected to lead the Attorney General's China Initiative, put in place to counter the Peoples Republic of China's persistent and aggressive economic espionage, trade secret theft, hacking and other related crimes.

Prior to rejoining the Department, John was Vice President and Assistant General Counsel at The Boeing Company, where he held several senior positions including in Boeing Defense, Space, and Security and as lead lawyer and head of international government affairs for Boeing International.

From 2006 to 2009, John served on the first leadership team of the National Security Division, first as Senior Counsel to the Assistant Attorney General and then as Deputy Assistant Attorney General for the Office of Law & Policy. In addition, he has served in the Office of Legal Counsel and the Office of the Deputy Attorney General. From 2010 to 2017, he taught national security law as an adjunct professor at the Georgetown University Law Center. John worked in private practice in Boston and clerked for Associate Justice Antonin Scalia of the U.S. Supreme Court and Judge Diarmuid O'Scannlain of the U.S. Court of Appeals for the Ninth Circuit. He graduated from Harvard Law School and the College of the Holy Cross.

China-Related Cases since January 2018

Tuesday, July 2, 2019

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

An electrical engineer has been found guilty of multiple federal criminal charges, including engaging in a scheme to illegally obtain integrated circuits with military applications that later were exported to China without the required export license. Assistant Attorney General for National Security John C. Demers, U.S. Attorney Nicola T. Hanna for the Central District of California and Assistant Director in Charge Paul Delacourt of the FBI's Los Angeles Field Office made the announcement.

After a six-week trial, Yi-Chi Shih, 64, a part-time Los Angeles resident, was found guilty on June 26 of conspiracy to violate the International Emergency Economic Powers Act (IEEPA), a federal law that makes illegal, among other things, certain unauthorized exports. The jury also found Shih guilty of mail fraud, wire fraud, subscribing to a false tax return, making false statements to a government agency and conspiracy to gain unauthorized access to a protected computer to obtain information. Shih was convicted of all 18 counts in a federal grand jury indictment.

United States District Judge Kronstadt, who presided over a trial that spanned seven weeks in Los Angeles, California, decided on Monday that he will later consider the forfeiture allegations in the indictment, where the government is seeking that Shih should forfeit hundreds of thousands of dollars. Judge Kronstadt discharged the jury that previously had been scheduled today to consider forfeiture allegations against Shih.

United States District Judge John A. Kronstadt will also schedule a sentencing hearing, where Shih faces a statutory maximum sentence of 219 years in federal prison.

"The Department's China Initiative is focused on preventing and prosecuting thefts of American technology and intellectual property for the benefit of China," said Assistant Attorney General Demers. "The defendant has been found guilty of conspiring to export sensitive semiconductor chips with military applications to China. I would like to thank the prosecutors and agents, including those from the Royal Canadian Mounted Police, for theirs efforts in this successful investigation and prosecution."

"This defendant schemed to export to China semiconductors with military and civilian uses, then he lied about it to federal authorities and failed to report income generated by the scheme on his tax returns," said United States Attorney Nick Hanna. "My office will enforce laws that protect our nation's intellectual property from being used to benefit foreign adversaries who may compromise our national security."

"The FBI is committed to protecting institutions from adversaries who seek to steal sensitive American technology under the guise of research," said Assistant Director in Charge Delacourt. "We will continue to work collaboratively with our federal partners to identify and hold accountable individuals who plunder our research or intellectual property at the expense of the American people and our national security."

According to the evidence presented at trial, Shih and co-defendant Kiet Ahn Mai, 65, of Pasadena, California, conspired to illegally provide Shih with unauthorized access to a protected computer of a United States company that manufactured wide-band, high-power semiconductor chips known as monolithic microwave integrated circuits (MMICs).

Shih defrauded the U.S. company out of its proprietary, export-controlled items, including its design services for MMICs, according to trial evidence. As part of the scheme, Shih accessed the victim company's computer systems via its web portal after Mai obtained that access by posing as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih and Mai concealed Shih's true intent to transfer the U.S. company's products to the People's Republic of China. The MMICs that Shih sent to China required a license from the Commerce Department before being exported to China, and a license was never sought or obtained for this export.

The victim company's semiconductor chips have a number of commercial and military applications, and its customers include the Air Force, Navy and the Defense Advanced Research Projects Agency. MMICs are used in missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures and radar applications.

The semiconductor chips at the heart of this case were shipped to Chengdu GaStone Technology Company (CGTC), a Chinese company that was building a MMIC manufacturing facility in Chengdu. Shih was the president of CGTC, which in 2014 was placed on the Commerce Department's Entity List, according to court documents, "due to its involvement in activities contrary to the national security and foreign policy interest of the United States – specifically, that it had been involved in the illicit procurement of commodities and items for unauthorized military end use in China."

Shih used a Hollywood Hills-based company he controlled – Pullman Lane Productions LLC – to funnel funds provided by Chinese entities to finance the manufacturing of MMICs by the victim company. Pullman Lane received financing from a Beijing-based company that was placed on the Entity List the same day as CGTC "on the basis of its involvement in activities contrary to the national security and foreign policy interests of the United States," according to court documents.

Shih and Mai were indicted in this case in January 2018. Mai pleaded guilty in December 2018 to one felony count of smuggling and is scheduled to be sentenced on September 19, at which time he will face a statutory maximum sentence of 10 years in federal prison.

This case was investigated by the Federal Bureau of Investigation; the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and IRS Criminal Investigation, with assistance from the Royal Canadian Mounted Police.

The matter is being prosecuted by Assistant United States Attorneys Judith A. Heinz, Melanie Sartoris, Khaldoun Shobaki and William Rollins of the National Security Division, Assistant United States Attorney James C. Hughes of the Major Frauds Section, Assistant United States Attorney John J. Kucera of the Asset Forfeiture Section, and Trial Attorney Matthew Walczewski of the Department of Justice's National Security Division.

Friday, May 17, 2019

Former CIA Officer Sentenced to Prison for Espionage

Kevin Patrick Mallory, 62, of Leesburg, Virginia, was sentenced today to 20 years in prison to be followed by five years of supervised release after being convicted under the Espionage Act for conspiracy to transmit national defense information to an agent of the People's Republic of China. Assistant Attorney General for National Security John C. Demers, U.S. Attorney G. Zachary Terwilliger for the Eastern District of Virginia and Assistant Director in Charge Nancy McNamara of the FBI's Washington Field Office made the announcement after sentencing by Senior U.S. District Judge T.S. Ellis III.

"Former U.S. Intelligence officer Kevin Patrick Mallory will spend the next 20 years of his life in prison for conspiring to pass national defense information to a Chinese intelligence officer," said Assistant Attorney General John Demers. "This case is one in an alarming trend of former U.S. intelligence officers being targeted by China and betraying their country and colleagues. This sentence, together with the recent guilty pleas of Ron Hansen in Utah and Jerry Lee in Virginia, deliver the stern message that our former intelligence officers have no business partnering with the Chinese, or any other adversarial foreign intelligence service."

"Mallory not only put our country at great risk, but he endangered the lives of specific human assets who put their own safety at risk for our national defense," said. U.S. Attorney Terwilliger. "There are few crimes in this country more serious than espionage, and this office has a long history of holding accountable those who betray our country. As the Chinese continue to attempt to identify and recruit current and former members of the United States intelligence community, those individuals should remain vigilant and report any suspicious activity to the appropriate security officials. This case should send a message to anyone considering violating the public's trust and compromising our national security by disclosing classified information. We will remain steadfast and dogged in pursuit of these challenging but critical national security cases."

"U.S. Government employees are trusted to keep the nation's secrets safe," said Assistant Director in Charge McNamara, "and this case shows the violation of that trust and duty will not be accepted. The targeting of former U.S. security clearance holders by foreign intelligence services is a constant threat we face, and the FBI will continue to preserve and combat these threats head on. I would like to thank the men and women of the FBI, and our counterparts at the Department of Justice, for their years of hard work to investigate and prosecute this case."

Mallory was found guilty by a federal jury in June 2018 of conspiracy to deliver, attempted delivery, delivery of national defense information to aid a foreign government and

making material false statements. The district court subsequently ordered acquittal as to the delivery and attempted delivery of national defense information counts due to lack of venue.

According to court records and evidence presented at trial, in March and April 2017, Mallory, a former U.S. intelligence officer, travelled to Shanghai to meet with an individual, Michael Yang, who held himself out as a People's Republic of China think tank employee, but whom Mallory assessed to be a Chinese Intelligence Officer.

Mallory, a United States citizen who speaks fluent Mandarin Chinese, consented to an FBI review of a covert communications (covcom) device he had been given by Yang to facilitate covert communications between the two. Analysis of the device, which was a Samsung Galaxy smartphone, revealed a number of communications in which Mallory and Yang talked about classified information that Mallory could sell to the PRC's intelligence service. FBI analysts were able to determine that Mallory had completed all of the steps necessary to securely transmit at least five classified U.S. government documents via the covcom device, one of which contained unique identifiers for human sources who had helped the United States government. At least two of the documents were successfully transmitted, and Mallory and Yang communicated about those two documents on the covcom device.

Evidence presented at trial included surveillance video from a FedEx store in Leesburg where Mallory could be seen scanning documents classified at the Secret and Top Secret level onto a micro SD card. Though Mallory paid to have the paper copies of the eight documents shredded, FBI agents found a carefully concealed SD card containing those documents during a search of Mallory's home, the day of his June 22, 2017 arrest. A recording was played at trial from June 24, 2017, where Mallory could be heard on a call from the jail asking his family to search for the hidden SD card.

Mallory has held numerous positions with various government agencies and several defense contractors, including working as a covert case officer for the Central Intelligence Agency (CIA) and an intelligence officer for the Defense Intelligence Agency (DIA). As required for his various government positions, Mallory obtained a Top Secret security clearance, which was active during various assignments during his career. Mallory's security clearance was terminated in October 2012 when he left government service.

Assistant U.S. Attorneys John T. Gibbs and Colleen E. Garcia, and Trial Attorneys Jennifer Kennedy Gellie and Evan Turgeon of the National Security Division's Counterintelligence and Export Control Section prosecuted the case.

Wednesday, May 1, 2019

Former CIA Officer Pleads Guilty to Conspiracy to Commit Espionage

A former Central Intelligence Agency (CIA) case officer pleaded guilty today to conspiring to communicate, deliver and transmit national defense information to the People's Republic of China. Assistant Attorney General for National Security John C. Demers, U.S. Attorney G. Zachary Terwilliger for the Eastern District of Virginia, Assistant Director for Counterintelligence John Brown of the FBI and Assistant Director in Charge Nancy McNamara of the FBI's Washington Field Office made the announcement after Senior U.S. District Judge T.S. Ellis III accepted the plea.

According to court documents, Jerry Chun Shing Lee, 54, left the CIA in 2007 and began residing in Hong Kong. In April 2010, two Chinese intelligence officers (IOs) approached Lee and offered to pay him for national defense information he had acquired as a CIA case officer. The IOs also told Lee they had prepared for him a gift of $100,000 cash, and they offered to take care of him "for life" in exchange for his cooperation.

Beginning sometime in May 2010 and continuing into at least 2011, Lee received requests for information, or taskings, from the Chinese IOs. The majority of the taskings asked Lee to reveal sensitive information about the CIA, including national defense information. On May 14, 2010, Lee made or caused to be made a cash deposit of $138,000 HKD (approximately $17,468 in USD) into his personal bank account in Hong Kong. This would be the first of hundreds of thousands of dollars (USD equivalent) in cash deposits Lee made or caused to be made into his personal HSBC account from May 2010 through December 2013.

"This is the third case in less than a year in which a former US intelligence officer has pled or been found guilty of conspiring with Chinese intelligence services to pass them national defense information," said Assistant Attorney General Demers. "Every one of these cases is a tragic betrayal of country and colleagues. The National Security Division will continue to prosecute individuals like Lee who abuse their former access to classified information for financial gain while threatening the security of America. Many thanks to the agents, analysts and prosecutors whose work led to today's outcome."

"Those Americans entrusted with our government's most closely held secrets have a tremendous responsibility to safeguard that information," said U.S. Attorney Terwilliger. "Instead of embracing that responsibility and honoring his commitment to not disclose national defense information, Lee sold out his country, conspired to become a spy for a foreign government, and then repeatedly lied to investigators about his conduct. This prosecution should serve as a warning to others who would compromise our nation's secrets and betray our country's trust. My thanks to the prosecutors, agents and our intelligence community partners for their terrific work on this important case."

"Today, Mr. Lee accepts responsibility not only for his crimes but also for their dangerous ramifications" said Assistant Director Brown. "By knowingly aiding a foreign government, Mr. Lee put our country's national security at serious risk and also threatened the safety and personal security of innocent people, namely his former intelligence colleagues. He deserves to answer for his treachery and he will do so as a result of the dedication of the FBI's Counterintelligence Division, the Washington Field Office, and the Department of Justice in pursuing this case."

"Today's guilty plea is an example of how the FBI and the Department of Justice successfully pursue threats to our nation's security and intelligence," said Assistant Director McNamara. "U.S. Government employees are entrusted by the American people to keep our country safe and secure from adversaries. The targeting of former U.S. security clearance holders by Chinese intelligence services is a constant threat we face, and the FBI will continue to combat these threats and guard our nation against those who conspire to compromise our national security. I would like to thank the hardworking people of the FBI who work each day to defend our security and intelligence."

On May 26, 2010, Lee created on his laptop computer a document that described, among other things, certain locations to which the CIA would assign officers with certain identified

experience, as well as the particular location and timeframe of a sensitive CIA operation. After Lee created this document, he transferred it from his laptop to a thumb drive. The document included national defense information of the United States that was classified at the Secret level.

In August 2012, the FBI conducted a court-authorized search of a hotel room in Honolulu, Hawaii registered in Lee's name. The search revealed that Lee possessed the thumb drive within his personal luggage. The FBI forensically imaged the thumb drive and later located the document in the unallocated space of the thumb drive, meaning that it had been deleted. The search also revealed that Lee possessed a day planner and an address book that contained handwritten notes made by Lee that related to his work as a CIA case officer prior to 2004. These notes included, among other things, intelligence provided by CIA assets, true names of assets, operational meeting locations and phone numbers, and information about covert facilities.

During 2012, Lee had a series of interviews with the CIA. Throughout these interviews, in response to questions about what the IOs had wanted from him, Lee intentionally failed to disclose that he had received taskings from them. In May 2013, the FBI conducted three interviews with Lee. During one of those interviews, Lee admitted that he had received taskings but stated that he had not kept the written requests because they would tend to incriminate him.

The FBI interviewers also confronted Lee with the sensitive document discovered on the thumb drive. Lee falsely denied that he possessed it, claimed not to know who created it, and denied knowing why it would have been on his computer. He also denied deleting the document. Approximately one week later, in another FBI interview, Lee admitted that he created the document in response to two taskings from the IOs and transferred it to a thumb drive. He also said he thought about giving it to the IOs but never did.

In a January 2018 interview with the FBI, Lee falsely denied that he ever kept any work-related notes at home. When shown a photocopy of the front covers of the day planner and address book described above, as well as a copy of his handwriting therein, Lee falsely denied that he possessed the notebooks while transiting through Hawaii in August 2012. Lee also falsely denied that either of the books contained notes from asset meetings but conceded that any such notes would be classified. Further, Lee falsely denied that he ever put the sensitive document on a thumb drive, notwithstanding the fact that he had admitted having done so when interviewed by FBI agents in May 2013. Finally, Lee also falsely told the interviewing agents that in drafting this document he was writing down things "more [like] a diary thing," notwithstanding the fact that in May 2013 he had told FBI agents that he had created the document in response to two taskings from the Chinese IOs.

Lee pleaded guilty to conspiracy to deliver national defense information to aid a foreign government and faces a maximum penalty of life in prison when sentenced on Aug. 23, 2019. Actual sentences for federal crimes are typically less than the maximum penalties. A federal district court judge will determine any sentence after taking into account the U.S. Sentencing Guidelines and other statutory factors.

Assistant U.S. Attorney Neil Hammerstrom and Trial Attorneys Patrick T. Murphy and Adam L. Small of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case, with assistance from Assistant U.S. Attorney Inayat Delawala.

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

Candace Marie Claiborne, a former employee of the U.S. Department of State, pleaded 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.

The announcement was made by Assistant Attorney General for National Security John C. Demers, U.S. Attorney Jessie K. Liu of the District of Columbia, Assistant Director in Charge Nancy McNamara of the FBI's Washington Field Office and Deputy Assistant Secretary Ricardo Colón, Domestic Operations, U.S. Department of State's Diplomatic Security Service.

The plea took place before the Honorable Randolph D. Moss of the U.S. District Court for the District of Columbia.

"Candace Marie Claiborne traded her integrity and non-public information of the United States government in exchange for cash and other gifts from foreign agents she knew worked for the Chinese intelligence service," said Assistant Attorney General Demers. "She withheld information and lied repeatedly about these contacts. Violations of the public's trust are an affront to our citizens and to all those who honor their oaths. With this guilty plea we are one step closer to imposing justice for these dishonorable criminal acts."

"Candace Claiborne broke the public trust when she accepted gifts and money from foreign officials, and then lied about it to State Department background investigators," said U.S. Attorney Liu. "The United States will continue to seek to hold accountable those who abuse their positions of trust."

"Candace Claiborne was entrusted with Top Secret information when she purposefully misled federal investigators about her repeated interactions with foreign contacts which violated her oath of office as a State Department employee," said Assistant Director McNamara. "The FBI will continue to investigate individuals who fail to report foreign contacts, which is a key indicator of potential insider threats posed by those in positions of public trust."

"Our close working relationship with the FBI and the Department of Justice resulted in the conviction of Candace Claiborne who violated the public trust and damaged our national security," said Deputy Assistant Secretary Colón. "Diplomatic Security will continue working with our law enforcement partners to vigorously defend the interests and security of the United States of America."

According to the plea documents, Claiborne, 63, began working as an Office Management Specialist for the Department of State in 1999. She served overseas at a number of posts, including embassies and consulates in Baghdad, Iraq, Khartoum, Sudan, and Beijing and Shanghai, China. As a condition of her employment, Claiborne maintained a TOP SECRET security clearance. Claiborne also was required to report any contacts with persons suspected of affiliation with a foreign intelligence agency as well as any gifts she received from foreign sources over a certain amount.

Despite such a requirement, Claiborne failed to report repeated contacts with two agents of the People's Republic of China Intelligence Service, even though these agents provided tens of thousands of dollars in gifts and benefits to Claiborne and her family over five years. The gifts and benefits included cash wired to Claiborne's USAA account, Chinese New Year's gifts, international travel and vacations, tuition at a Chinese fashion school, a fully furnished apartment, a monthly stipend and numerous cash payments. Some of these gifts and benefits were provided directly to Claiborne, while others were provided to a close family member of Claiborne's.

In exchange for these gifts and benefits, as stated in the plea documents, Claiborne provided copies of internal documents from the State Department on topics ranging from U.S. economic strategies to visits by dignitaries between the two countries.

Claiborne noted in her journal that she could "Generate 20k in 1 year" working with one of the PRC agents. That same agent at one point tasked her with providing internal U.S. Government analyses on a U.S.-Sino Strategic Economic Dialogue that had just concluded.

Claiborne, who confided to a co-conspirator that the PRC agents were "spies," willfully misled State Department background investigators and FBI investigators about her contacts with those agents, the plea documents state. After the State Department and FBI investigators contacted her, Claiborne also instructed her co-conspirators to delete evidence connecting her to the PRC agents. She was arrested on March 28, 2017, following a law enforcement investigation.

Judge Moss scheduled sentencing for July 9, 2019. Claiborne, of Washington, D.C., was ordered detained pending sentencing, but will self-surrender for said detention on June 5, 2019. The statutory maximum penalty for a person convicted of conspiracy to defraud the United States is five years in prison. The maximum statutory sentences are prescribed by Congress and are provided here for informational purposes. The sentencing of the defendant will be determined by the court after considering the advisory Sentencing Guidelines and other statutory factors.

The FBI's Washington Field Office is leading the investigation into this matter. The case was prosecuted by Thomas A. Gillice and investigated by John L. Hill, both Assistant U.S. Attorneys in the U.S. Attorney's Office for the District of Columbia, and Deputy Chief Julie A. Edelstein and Trial Attorney Evan N. Turgeon of the National Security Division's Counterintelligence and Export Control Section.

Tuesday, April 23, 2019

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

An indictment unsealed today charges Xiaoqing Zheng, 56, of Niskayuna, New York, and Zhaoxi Zhang, 47, of Liaoning Province, China, 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. Assistant Attorney General for National Security John C. Demers, U.S. Attorney Grant C. Jaquith for the Northern District of New York, Assistant Director John Brown of the FBI's

Counterintelligence Division and Special Agent in Charge James N. Hendricks of the FBI's Albany Field Office made the announcement.

According to the 14-count indictment, Zheng, while employed at GE Power & Water in Schenectady, New York as an engineer specializing in sealing technology, exploited his access to GE's files by stealing multiple electronic files, including proprietary files involving design models, engineering drawings, configuration files, and material specifications having to do with various components and testing systems associated with GE gas and steam turbines. Zheng e-mailed and transferred many of the stolen GE files to his business partner, Chinese businessman Zhaoxi Zhang, who was located in China. Zheng and Zhang used the stolen GE trade secrets to advance their own business interests in two Chinese companies - Liaoning Tianyi Aviation Technology Co., Ltd. (LTAT) and Nanjing Tianyi Avi Tech Co. Ltd. (NTAT), companies which research, develop, and manufacture parts for turbines.

The indictment also alleges that Zheng and Zhang conspired to commit economic espionage, as the thefts of GE's trade secrets surrounding various turbine technologies were done knowing and intending that the thefts would benefit the People's Republic of China and one or more foreign instrumentalities, including LTAT, NTAT, Shenyang Aerospace University, Shenyang Aeroengine Research Institute, and Huaihai Institute of Technology. The defendants, through LTAT and NTAT, received financial and other support from the Chinese government and coordinated with Chinese government officials to enter into research agreements with Chinese state-owned institutions to develop turbine technologies.

"The indictment alleges a textbook example of the Chinese government's strategy to rob American companies of their intellectual property and to replicate their products in Chinese factories, enabling Chinese companies to replace the American company first in the Chinese market and later worldwide," said Assistant Attorney General Demers. "We will not stand idly by while the world's second-largest economy engages in state-sponsored theft. As part of the Attorney General's China Initiative, we will partner with the private sector to hold responsible those who violate our laws, and we urge China's leaders to join responsible nations and to act with honesty and integrity when competing in the global marketplace."

"As alleged, the thefts of trade secrets to benefit the People's Republic of China are serious crimes against the victimized company and our country," said U.S. Attorney Jaquith. "Both fair competition and incentivized innovation require that American companies be able to rely on the secrecy of technological advances forged through their talent and tenacity. When technology is taken through treachery, we will continue to work with the National Security Division and the FBI to prosecute the perpetrators."

"American businesses spend many hours and large amounts of money developing unique technology. When such technology is stolen it can be devastating to U.S. businesses and can result in American workers losing jobs," said FBI Assistant Director Brown. "China continues to support behavior that violates the rule of law. This case demonstrates the FBI will continue to pursue China's efforts to steal American technology."

"Economic espionage and the theft of trade secrets have a profound impact on our companies and communities," said FBI Special Agent in Charge Hendricks. "We view this as a grave threat to our economic and national security and the FBI will work tirelessly to prevent the loss of American technology and American jobs."

Zheng was arraigned today in Albany, New York, before United States Magistrate Judge Christian F. Hummel, and released with conditions pending a trial before United States District Judge Mae A. D'Agostino.

The economic espionage counts (Counts One, Three, Four, Seven, Eight and Eleven) carry a maximum sentence of 15 years in prison, a fine of up to $5,000,000, and a term of supervised release of up to three years. The trade secrets theft counts (Counts Two, Five, Six, Nine, Ten, Twelve and Thirteen) carry a maximum sentence of 10 years in prison, a fine of up to $250,000, and a term of supervised release of up to three years. Count Fourteen of the indictment, which charges Zheng with making false statements to the FBI during a voluntary interview, carries a maximum sentence of 5 years in prison, a fine of up to $250,000, and a term of supervised release of up to three years.

The charges in the indictment are merely accusations. The defendants are presumed innocent unless and until proven guilty.

This case is being investigated by the Federal Bureau of Investigation, and is being prosecuted by Assistant U.S. Attorney Rick Belliss, and National Security Division Trial Attorneys Jason McCullough and Matthew Chang.

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

Earlier today, in federal court in Brooklyn, New York, Ying Lin pleaded guilty to acting as an agent of the People's Republic of China (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, a former manager with an international air carrier headquartered in the PRC (the Air Carrier), abused her privileges to transport packages from John F. Kennedy International Airport (JFK Airport) to the PRC aboard Air Carrier flights at the behest of the PRC military officers and in violation of Transportation Security Administration (TSA) regulations. The proceeding was held before United States District Judge Ann M. Donnelly.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney Richard P. Donoghue for the Eastern District of New York, Assistant Director in Charge William F. Sweeney, Jr of the FBI's New York Field Office, and Special Agent in Charge Angel M. Melendez, Department of Homeland Security, Homeland Security Investigations (HSI) announced the guilty plea.

"This case is a stark example of the Chinese government using the employees of Chinese companies doing business here to engage in illegal activity," said Assistant Attorney General Demers. "Covertly doing the Chinese military's bidding on U.S. soil is a crime, and Lin and the Chinese military took advantage of a commercial enterprise to evade legitimate U.S. government oversight."

"The defendant's actions as an agent of the Chinese government helped Chinese military officers to evade U.S. law enforcement scrutiny of packages that they sent from New York to

Beijing," stated United States Attorney Donoghue. "This case demonstrates how seriously we address counterintelligence threats posed by individuals in the United States who work for foreign governments, such as China."

"The FBI and our law enforcement partners do all we can every day to protect this country from the threats we can see, and we work even harder to find the threats we can't see," said FBI Assistant Director-in-Charge Sweeney. "Ms. Lin was secreting packages through some of the country's busiest airports, using her work with the Chinese government to thwart our security measures. We believe this case isn't unique and hope it serves as an example that the Chinese and other foreign governments can't break our laws with impunity."

"Lin's criminal actions exploited the international boundary of the United States as she used her position to smuggle packages onto planes headed to China," said HSI Special Agent-in-Charge Melendez. "We are committed to ensuring the integrity of our international airports so they are not used as a front for illicit activities."

Lin worked for the Air Carrier from 2002 through the fall of 2015 as a counter agent at JFK Airport and from the fall of 2015 through April 2016 as the station manager at Newark Liberty International Airport. During her employment with the Air Carrier, Lin accepted packages from the PRC military officers, and placed those packages aboard Air Carrier flights to the PRC as unaccompanied luggage or checked in the packages under the names of other passengers flying on those flights. As the PRC military officers did not travel on those flights, Lin's actions were contrary to a security program that required that checked baggage be accepted only from ticketed passengers, thereby violating TSA regulations. In addition, Lin encouraged other Air Carrier employees to assist the PRC military officers, instructing those employees that because the Air Carrier was a PRC company, their primary loyalty should be to the PRC.

In exchange for her work at the direction and under the control of PRC military officers and other PRC government officials, Lin received benefits from the PRC Mission and PRC Consulate in New York. These benefits included tax-exempt purchases of liquor, cigarettes and electronic devices worth tens of thousands of dollars. These benefits also included free contracting work at the defendant's two residences in Queens, New York, by PRC construction workers who were permitted under the terms of their visas to work only on PRC government facilities.

When sentenced, Lin faces up to 10 years' imprisonment. As part of the guilty plea, Lin agreed to forfeit approximately $25,000 as well as an additional $145,000 in connection with her resolution of the government's forfeiture verdict in United States v. Zhong, No. 16-CR-614 (AMD).

Mr. Demers and Mr. Donoghue expressed their appreciation to the Transportation Security Administration for their assistance on the case. The government's case is being handled by the National Security and Cybercrime Section. Assistant United States Attorneys Douglas M. Pravda, Alexander A. Solomon, Ian C. Richardson and Sarah M. Evans are in charge of the prosecution, with assistance from Trial Attorney Matthew R. Walczewski of the Department of Justice's Counterintelligence and Export Control Section. The forfeiture aspect of the case is being handled by EDNY Assistant United States Attorney Brian Morris of the Office's Civil Division.

Friday, March 15, 2019

Former Defense Intelligence Officer Pleads Guilty to Attempted Espionage

Ron Rockwell Hansen, 58, a resident of Syracuse, Utah, and a former Defense Intelligence Agency (DIA) officer, pleaded guilty today in the District of Utah in connection with his attempted transmission of national defense information to the People's Republic of China. Sentencing is set for Sept. 24, 2019.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney John Huber for the District of Utah and Special Agent in Charge Paul Haertel of the FBI's Salt Lake City Field Office announced the charges.

Hansen retired from the U.S. Army as a Warrant Officer with a background in signals intelligence and human intelligence. He speaks fluent Mandarin-Chinese and Russian. DIA hired Hansen as a civilian intelligence case officer in 2006. Hansen held a Top Secret clearance for many years, and signed several non-disclosure agreements during his tenure at DIA and as a government contractor.

As Hansen admitted in the plea agreement, in early 2014, agents of a Chinese intelligence service targeted Hansen for recruitment and he began meeting with them regularly in China. During those meetings, the Chinese agents described to Hansen the type of information that would interest the Chinese intelligence service. During the course of his relationship with the agents of the Chinese intelligence service, Hansen received hundreds of thousands of dollars in compensation for information he provided them, including information he gathered at various industry conferences. Between May 24, 2016 and June 2, 2018, Hansen solicited from an intelligence case officer working for the DIA national defense information that Hansen knew the Chinese intelligence service would find valuable. Hansen agreed to act as a conduit to sell that information to the Chinese. Hansen advised the DIA case officer how to record and transmit classified information without detection, and explained how to hide and launder any funds received as payment for classified information. The DIA case officer reported Hansen's conduct to the DIA and subsequently acted as a confidential human source for the FBI.

As Hansen further admitted in the plea agreement, Hansen met with the DIA case officer on June 2, 2018, and received from that individual documents containing national defense information that Hansen previously solicited. The documents Hansen received were classified. The information in the documents related to the national defense of the United States in that it related to United States military readiness in a particular region and was closely held by the United States government. Hansen reviewed the documents, queried the DIA case officer about their contents, and took written notes about the materials relating to the national defense information. Hansen advised the DIA case officer that he would remember most of the details about the documents he received that day and would conceal some notes about the material in the text of an electronic document that Hansen would prepare at the airport before leaving for China. Hansen intended to provide the information he received to the agents of the Chinese intelligence service with whom he had been meeting, and Hansen knew that the information was to be used to the injury of the United States and to the advantage of a foreign nation.

Hansen pleaded guilty to one count of attempting to gather or deliver national defense information to aid a foreign government. The plea agreement calls for an agreed-upon sentence of 15 years.

Special agents of the FBI, IRS, U.S. Department of Commerce, the Department of Defense, U.S. Army Counterintelligence, and the Defense Intelligence Agency were involved in the investigation.

The prosecution was handled by Assistant U.S. Attorneys Robert A. Lund, Karin Fojtik, Mark K. Vincent and Alicia Cook of the District of Utah, and Trial Attorneys Patrick T. Murphy, Matthew J. McKenzie and Adam L. Small of the National Security Division's Counterintelligence and Export Control Section. Prosecutors from the U.S. Attorney's Office for the Western District of Washington assisted with this case.

Friday, February 15, 2019

Chinese National Sentenced to Prison for Selling Counterfeit Computer Parts

A Beijing, China man was sentenced today to 54 months in federal prison for directing the shipment of counterfeit computer-networking equipment into the Southern District of Texas.

Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division and U.S. Attorney Ryan K. Patrick for the Southern District of Texas made the announcement.

Ruiyang Li, 40, was sentenced today to serve 54 months in federal prison by U.S. District Judge Ewing Werlein Jr. The court reserved the determination of restitution to the victims of Li's trademark counterfeiting—including Cisco Systems Inc., The Hewlett-Packard Company and Intel Corporation—until a later date. Because Li is not a U.S. citizen, he is expected to be deported after serving his prison sentence.

From at least 2007 until in or about June 2017, Li directed the shipment of counterfeit computer-networking equipment into the Southern District of Texas, first when selling to a retailer in Magnolia, Texas, and eventually when selling to law enforcement acting in an undercover capacity. Over this time period, Li sold counterfeit networking products through several business entities, often hiding behind layers of personal and corporate aliases to evade detection by law enforcement. Li also used various means to conceal his unlawful conduct, including by sending and receiving payments using accounts that did not appear connected, at least publicly, to companies trafficking in illicit products. Li and his customers would also agree to mislabel packages, break up shipments into separate components, alter destination addresses and use multiple forwarding companies based in the United States. These methods, in Li's mind, made shipping counterfeit parts "safer," which in practice meant delaying or complicating detection by U.S. authorities.

State and local governments rely on complex computer networking technology, including the transceivers and other parts that were trafficked in this case, to manage critical data and operations. This same technology is also prominent in banks, hospitals, air traffic control installations, power plants and other essential infrastructure. Because counterfeit parts are often not subject to stringent manufacturing requirements, they present a significant health and safety risk to communities across the United States.

The case was investigated by U.S. Immigration and Customs Enforcement's Homeland Security Investigations, with significant assistance from U.S. Customs and Border Protection. The case was prosecuted by Senior Trial Attorney Timothy C. Flowers of the Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Jay Hileman.

Thursday, February 14, 2019

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

A grand jury sitting in Greeneville, Tennessee has returned an indictment against Xiaorong You, a/k/a Shannon You, 56, of Lansing, Michigan, and Liu Xiangchen, 61, of Shandong Province, China 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.

Assistant Attorney General National Security John C. Demers, U.S. Attorney J. Douglas Overbey of the Eastern District of Tennessee, FBI Executive Assistant Director for the National Security Branch Jay Tabb, and Special Agent in Charge Troy Sowers of the FBI's Knoxville Field Office made the announcement.

"The conduct alleged in today's indictment exemplifies the rob, replicate and replace approach to technological development," said Assistant Attorney General Demers. "Xiaorong You is accused of an egregious, premediated theft and transfer of trade secrets worth more than $100 million for the purpose of setting up a Chinese company that would compete with the American companies from which the trade secrets were stolen. Unfortunately, China continues to use its national programs, like the 'Thousand Talents,' to solicit and reward the theft of our nation's trade secrets and intellectual property, but the Justice Department will continue to prioritize investigations like these, to ensure that China understands that this criminal conduct is not an acceptable business or economic development practice."

"Our office is committed to working closely with our federal, state and local partners to identify and prosecute those who engage in illegal and deceptive practices to steal trade secret and protected information from companies who spend millions of dollars to develop it," said U.S. Attorney Overbey. "Not only can theft of this information be potentially devastating to our American companies, it could also pose a threat to our overall national and economic security."

"The facts laid out in this indictment show the conspirators engaged in blatant criminal activity," said Executive Assistant Director Tabb. "They didn't stop at going after technical secrets belonging to just one company. They allegedly targeted multiple companies and made off with trade secrets at an estimated value of almost 120 million dollars. As this case demonstrates, the FBI is determined to do everything possible to bring to justice those who try to steal secrets belonging to American companies."

"As this indictment highlights, theft of trade secrets from American companies is an emerging economic threat, even here in East Tennessee," said Special Agent in Charge Sowers. "The tireless work of our agents and prosecutors in this case underscores the FBI's commitment to protecting American ingenuity."

The BPA-free trade secrets allegedly stolen by these individuals belonged to multiple owners and cost an estimated total of at least $119,600,000 to develop. Until recently, bisphenol-A (BPA) was used to coat the inside of cans and other food and beverage containers to help minimize flavor loss, and prevent the container from corroding or reacting with the food or beverage contained therein. However, due to the discovered potential harmful effects of BPA, companies began searching for BPA-free alternatives. These alternatives are difficult and expensive to develop.

From December 2012 through Aug. 31, 2017, You was employed as Principal Engineer for Global Research by a company in Atlanta, which had agreements with numerous companies to conduct research and development, testing, analysis and review of various BPA-free technologies. Due to her extensive education and experience with BPA and BPA-free coating technologies, she was one of a limited number of employees with access to trade secrets belonging to the various owners. From approximately September 2017 through June 2018, You was employed as a packaging application development manager for a company in Kingsport, Tennessee, where she was one of a limited number of employees with access to trade secrets belonging to that company.

Details of the conspiracy are included in the indictment on file with the U.S. District Court. The indictment alleges that You, Liu, and a third co-conspirator formulated a plan in which You would exploit her employment with the two American employers to steal trade secrets and provide the information for the economic benefit of trade secrets the Chinese company that Liu managed, which would manufacture and profit from products developed using the stolen trade secrets. In exchange, Liu would cause the Chinese company to reward You for her theft, by helping her receive the Thousand Talent and another financial award, based on the trade secrets she stole, and by giving You an ownership share of a new company that would "own" the stolen trade secrets in China. The conspirators also agreed to compete with U.S. and foreign companies, including some of the owners of the stolen stolen trade secrets, in China and elsewhere, by selling products designed, developed and manufactured using the stolen trade secrets.

The charges contained in this indictment are merely allegations, and the defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

The case is being investigated by the FBI's Knoxville Field Office.

The government's case is being prosecuted by the Eastern District of Tennessee and the National Security Division's Counterintelligence and Export Control Section.

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

A 10-count indictment unsealed today in the Western District of Washington State charges 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 Bellevue, Washington based 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.

"Today we are announcing that we are bringing criminal charges against telecommunications giant Huawei and its associates for nearly two dozen alleged crimes" Acting Attorney General Matthew G. Whitaker said. "As I told Chinese officials in August, China must

hold its citizens and Chinese companies accountable for complying with the law. I'd like to thank the many dedicated criminal investigators from several different federal agencies who contributed to this investigation and the Department of Justice attorneys who are moving the prosecution efforts forward. They are helping us uphold the rule of law with integrity."

"The charges unsealed today clearly allege that Huawei intentionally conspired to steal the intellectual property of an American company in an attempt to undermine the free and fair global marketplace," said FBI Director Wray. "To the detriment of American ingenuity, Huawei continually disregarded the laws of the United States in the hopes of gaining an unfair economic advantage. As the volume of these charges prove, the FBI will not tolerate corrupt businesses that violate the laws that allow American companies and the United States to thrive."

"This indictment shines a bright light on Huawei's flagrant abuse of the law – especially its efforts to steal valuable intellectual property from T-Mobile to gain unfair advantage in the global marketplace," said First Assistant U.S. Attorney Annette L. Hayes of the Western District of Washington. "We look forward to presenting the evidence of Huawei's crimes in a court of law, and proving our case beyond a reasonable doubt. Fair competition and respect for the rule of law is essential to the functioning of our international economic system."

According to the indictment, in 2012 Huawei began a concerted effort to steal information on a T-Mobile phone-testing robot dubbed "Tappy." In an effort to build their own robot to test phones before they were shipped to T-Mobile and other wireless carriers, Huawei engineers violated confidentiality and non-disclosure agreements with T-Mobile by secretly taking photos of "Tappy," taking measurements of parts of the robot, and in one instance, stealing a piece of the robot so that the Huawei engineers in China could try to replicate it. After T-Mobile discovered and interrupted these criminal activities, and then threatened to sue, Huawei produced a report falsely claiming that the theft was the work of rogue actors within the company and not a concerted effort by Huawei corporate entities in the United States and China. As emails obtained in the course of the investigation reveal, the conspiracy to steal secrets from T-Mobile was a company-wide effort involving many engineers and employees within the two charged companies.

As part of its investigation, FBI obtained emails revealing that in July 2013, Huawei offered bonuses to employees based on the value of information they stole from other companies around the world, and provided to Huawei via an encrypted email address.

Under the maximum sentencing provisions applicable to corporate entities, Conspiracy and Attempt to Commit Trade Secret Theft are punishable by a fine of up to $5,000,000 or three times the value of the stolen trade secret, whichever is greater. Wire Fraud and Obstruction of Justice are punishable by a fine of up to $500,000.

The charges contained in the indictment are only allegations. A defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, the sentencing of the defendants will be determined by the court based on the advisory Sentencing Guidelines and other statutory factors.

The case is being investigated by the FBI. The case is being prosecuted by Assistant U.S. Attorneys Todd Greenberg and Thomas Woods of the Western District of Washington, with

assistance from the Department of Justice's National Security Division's Counterintelligence and Export Control Section.

U.S. Attorney Brian T. Moran has been recused from this matter because of legal representations he undertook before he joined the Department of Justice. Per direction from ethics officials in the Department of Justice, First Assistant U.S. Attorney Annette L. Hayes will act as U.S. Attorney with respect to this matter pursuant to the authority conferred by 28 U.S.C. § 515.

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

A 13-count indictment was unsealed earlier today in federal court in Brooklyn, New York, charging four defendants,[1] including Huawei Technologies Co. Ltd. (Huawei), the world's largest telecommunications equipment manufacturer, with headquarters in the People's Republic of China (PRC) and operations around the world. The indicted defendants include Huawei and two Huawei affiliates — Huawei Device USA Inc. (Huawei USA) and Skycom Tech Co. Ltd. (Skycom) — as well as Huawei's Chief Financial Officer (CFO) Wanzhou Meng (Meng).

The defendants 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.

Acting U.S. Attorney General Matthew G. Whitaker, Secretary Kirstjen Nielsen of the U.S. Department of Homeland Security, Secretary Wilbur Ross of the U.S. Department of Commerce, U.S. Attorney Richard P. Donoghue for the Eastern District of New York, FBI Director Christopher A. Wray, Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division and Assistant Attorney General John C. Demers of the National Security Division, announced the charges.

"Today we are announcing that we are bringing criminal charges against telecommunications giant Huawei and its associates for nearly two dozen alleged crimes," said Acting Attorney General Whitaker. "As I told Chinese officials in August, China must hold its citizens and Chinese companies accountable for complying with the law. I'd like to thank the many dedicated criminal investigators from several different federal agencies who contributed to this investigation and the Department of Justice attorneys who are moving the prosecution efforts forward. They are helping us uphold the rule of law with integrity."

"As charged in the indictment, Huawei and its Chief Financial Officer broke U.S. law and have engaged in a fraudulent financial scheme that is detrimental to the security of the

United States," said Secretary Nielsen. "They willfully conducted millions of dollars in transactions that were in direct violation of the Iranian Transactions and Sanctions Regulations, and such behavior will not be tolerated. The Department of Homeland Security is focused on preventing nefarious actors from accessing or manipulating our financial system, and we will ensure that legitimate economic activity is not exploited by our adversaries. I would like to thank ICE Homeland Security Investigations for their exceptional work on this case."

"For years, Chinese firms have broken our export laws and undermined sanctions, often using U.S. financial systems to facilitate their illegal activities," said Secretary Ross. "This will end. The Trump Administration continues to be tougher on those who violate our export control laws than any administration in history. I commend the Commerce Department's Office of Export Enforcement, and our partners in the FBI, Justice Department, Department of Defense, and Department of Homeland Security for their excellent work on this case."

"As charged in the indictment, Huawei and its subsidiaries, with the direct and personal involvement of their executives, engaged in serious fraudulent conduct, including conspiracy, bank fraud, wire fraud, sanctions violations, money laundering and the orchestrated obstruction of justice," stated U.S. Attorney Donoghue. "For over a decade, Huawei employed a strategy of lies and deceit to conduct and grow its business. This Office will continue to hold accountable companies and their executives, whether here or abroad, that commit fraud against U.S. financial institutions and their international counterparts and violate U.S. laws designed to maintain our national security." Mr. Donoghue thanked the FBI, U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI), U.S. Department of Commerce Office of Export Enforcement (OEE) and the Defense Criminal Investigative Service (DCIS) agents who are investigating this case for their tireless work and dedication.

"These charges lay bare Huawei's alleged blatant disregard for the laws of our country and standard global business practices," said FBI Director Wray. "Companies like Huawei pose a dual threat to both our economic and national security, and the magnitude of these charges make clear just how seriously the FBI takes this threat. Today should serve as a warning that we will not tolerate businesses that violate our laws, obstruct justice, or jeopardize national and economic well-being."

* * * *

Overview of the Indictment

The charges in this case relate to a long-running scheme by Huawei, its CFO, and other employees to deceive numerous global financial institutions and the U.S. government regarding Huawei's business activities in Iran. As alleged in the indictment, beginning in 2007, Huawei employees lied about Huawei's relationship to a company in Iran called Skycom, falsely asserting it was not an affiliate of Huawei. The company further claimed that Huawei had only limited operations in Iran and that Huawei did not violate U.S. or other laws or regulations related to Iran. Most significantly, after news publications in late 2012 and 2013 disclosed that Huawei operated Skycom as an unofficial affiliate in Iran and that Meng had served on the board of directors of Skycom, Huawei employees, and in particular Meng, continued to lie to Huawei's banking partners about Huawei's relationship with Skycom. They falsely claimed that Huawei had sold its interest in Skycom to an unrelated third party in 2007 and that Skycom was merely Huawei's local business partner in Iran. In reality, Skycom was Huawei's longstanding Iranian affiliate, and Huawei orchestrated the 2007 sale to appear as an arm's length transaction between

two unrelated parties, when in fact Huawei actually controlled the company that purchased Skycom.

As part of this scheme to defraud, Meng allegedly personally made a presentation in August 2013 to an executive of one of Huawei's major banking partners in which she repeatedly lied about the relationship between Huawei and Skycom.

According to the indictment, Huawei relied on its global banking relationships for banking services that included processing U.S.-dollar transactions through the United States. U.S. laws and regulations generally prohibited these banks from processing transactions related to Iran through the United States. The banks could have faced civil or criminal penalties for processing transactions that violated U.S. laws or regulations. Relying on the repeated misrepresentations by Huawei, these banks continued their banking relationships with Huawei. One bank cleared more than $100 million worth of Skycom-related transactions through the United States between 2010 and 2014.

In furtherance of this scheme to defraud, and as alleged in the indictment, Huawei and its principals repeatedly lied to U.S. government authorities about Huawei's business in Iran in submissions to the U.S. government, and in responses to government inquiries. For example, Huawei provided false information to the U.S. Congress regarding whether Huawei's business in Iran violated any U.S. law. Similarly, as indicated in the indictment, in 2007 — months before Huawei orchestrated the purported sale of Skycom to another Huawei-controlled entity — Huawei's founder falsely stated to FBI agents that Huawei did not have any direct dealings with Iranian companies and that Huawei operated in compliance with all U.S. export laws.

After one of Huawei's major global banking partners (identified as Financial Institution 1 in the indictment) decided to exit the Huawei relationship in 2017 because of Huawei's risk profile, Huawei allegedly made additional misrepresentations to several of its remaining banking partners in an effort to maintain and expand those relationships. Huawei and its principals are alleged to have repeatedly and falsely claimed that Huawei had decided to terminate its banking relationship with Financial Institution 1, when in fact it was Financial Institution 1 that had decided to terminate the banking relationship. Through these misrepresentations, Huawei was able to continue its banking relationships with its other banks.

In 2017, when Huawei became aware of the government's investigation, Huawei and its subsidiary Huawei USA allegedly tried to obstruct the investigation by making efforts to move witnesses with knowledge about Huawei's Iran-based business to the PRC, and beyond the jurisdiction of the U.S. government, and by concealing and destroying evidence of Huawei's Iran-based business that was located in the United States.

In December 2018, Canadian authorities apprehended Meng in Vancouver pursuant to a provisional arrest warrant issued under Canadian law. The U.S. government is seeking Meng's extradition to the United States.

The charges in the indictment are merely allegations, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

The indictment unsealed today is assigned to U.S. District Judge Ann M. Donnelly of the Eastern District of New York.

The government's investigation is ongoing.

The investigation is being jointly conducted by the FBI's New York Field Office, HSI's New York Field Office, OEE's New York Field Office, and DCIS's Southwest and Northeast Field Offices. Agents from the FBI, HSI, and OEE offices in Dallas provided significant support and assistance. The government's case is being handled by the National Security and Cybercrime and Business and Securities Fraud Sections of the U.S. Attorney's Office for the Eastern District of New York, the Justice Department's Criminal Division's Money Laundering and Asset Recovery Section (MLARS), and the Justice Department's National Security Division's Counterintelligence and Export Control Section (CES).

Assistant U.S. Attorneys Alexander A. Solomon, Julia Nestor, David K. Kessler, Kaitlin Farrell, and Sarah Evans, MLARS Trial Attorneys Laura Billings and Christian Nauvel, and CES Trial Attorneys Thea D. R. Kendler and David Lim are in charge of the prosecution, with assistance provided by Assistant U.S. Attorney Mark Penley of the Northern District of Texas, Assistant U.S. Attorneys Brian Morris and Brendan King of the Eastern District of New York's Civil Division and Trial Attorneys Andrew Finkelman and Margaret O'Malley of DOJ's Office of International Affairs. Additional Criminal Division and National Security Division Trial Attorneys and Assistant U.S. Attorneys within U.S. Attorney's Offices for the Northern District of Texas, the Eastern District of Texas, and the Northern District of California have provided valuable assistance with various aspects of this investigation.

The Defendants:

Huawei Technologies Co. Ltd.

Huawei Device USA Inc.

Skycom Tech Co. Ltd.

Meng Wanzhou, also known as "Cathy Meng" and "Sabrina Meng"

Age: 46

Residence: People's Republic Of China

E.D.N.Y. Docket No. 18-CR-457 (AMD)

[1] The indictment charges other individuals who have not yet been apprehended and whose names will not be publicly released at this time.

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

A federal jury in New York City today convicted the head of a nongovernmental organization (NGO) based in Hong Kong and Virginia 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, announced Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division and U.S. Attorney Geoffrey S. Berman of the Southern District of New York.

Chi Ping Patrick Ho, aka "Patrick C.P. Ho," aka "He Zhiping," 69, of Hong Kong, China, was found guilty today after a one-week jury trial before U.S. District Judge Loretta A. Preska in

the Southern District of New York of one count of conspiring to violate the Foreign Corrupt Practices Act (FCPA), four counts of violating the FCPA, one count of conspiring to commit international money laundering and one count of committing international money laundering. Ho is scheduled to be sentenced before Judge Preska on March 14, 2019, at 10:00 a.m. EDT.

"Patrick Ho paid millions of dollars in bribes to the leaders of two African countries to secure contracts for a Chinese conglomerate," said Assistant Attorney General Benczkowski. "Today's trial conviction demonstrates the Criminal Division's commitment to prosecuting those who seek to utilize our financial system to secure unfair competition advantages through corruption and bribery."

"Patrick Ho now stands convicted of scheming to pay millions in bribes to foreign leaders in Chad and Uganda, all as part of his efforts to corruptly secure unfair business advantages for a multibillion-dollar Chinese energy company," said U.S. Attorney Berman. "As the jury's verdict makes clear, Ho's repeated attempts to corrupt foreign leaders were not business as usual, but criminal efforts to undermine the fairness of international markets and erode the public's faith in its leaders."

According to evidence presented at trial, Ho was involved in two bribery schemes to pay top officials of Chad and Uganda in exchange for business advantages for CEFC China, a Shanghai-based multibillion-dollar conglomerate that operates internationally in multiple sectors, including oil, gas, and banking. At the center of both schemes was Ho, the head of a nongovernmental organization based in Hong Kong and Arlington, Virginia, the China Energy Fund Committee (the "CEFC NGO"), which held "Special Consultative Status" with the United Nations (UN) Economic and Social Council. CEFC NGO was funded by CEFC China.

According to the evidence presented at trial, in the first scheme (the "Chad Scheme"), Ho, on behalf of CEFC China, offered a $2 million cash bribe, hidden within gift boxes, to Idriss Déby, the President of Chad, in an effort to obtain valuable oil rights from the Chadian government. In the second scheme (the "Uganda Scheme"), Ho caused a $500,000 bribe to be paid, via wires transmitted through New York, New York, to an account designated by Sam Kutesa, the Minister of Foreign Affairs of Uganda, who had recently completed his term as the President of the UN General Assembly. Ho also schemed to pay a $500,000 cash bribe to Yoweri Museveni, the President of Uganda, and offered to provide both Kutesa and Museveni with additional corrupt benefits by "partnering" with them in future joint ventures in Uganda.

The Chad Scheme

According to the evidence presented at trial, the Chad Scheme began in or about September 2014 when Ho flew into New York, New York to attend the annual UN General Assembly. At that time, CEFC China was working to expand its operations to Chad and wanted to meet with President Déby as quickly as possible. Through a connection, Ho was introduced to Cheikh Gadio, the former Minister of Foreign Affairs of Senegal, who had a personal relationship with President Déby. Ho and Gadio met in midtown Manhattan, New York where Ho enlisted Gadio to assist CEFC China in obtaining access to President Déby.

Gadio connected Ho and CEFC China to President Déby. In an initial meeting in Chad in November 2014, President Déby described to Ho and CEFC China executives certain lucrative oil rights that were available for CEFC China to acquire. Following that meeting, Gadio advised

Ho and CEFC China to send a technical team to Chad to investigate the oil rights and make an offer to President Déby. Instead, Ho insisted on a prompt second meeting with the President. The second meeting took place a few weeks later, in December 2014. Ho led a CEFC China delegation, which flew into Chad on a corporate jet with $2 million cash concealed within several gift boxes. At the conclusion of a business meeting with President Déby, Ho and the CEFC China executives presented President Déby with the gift boxes.

To the surprise of Ho and the CEFC China executives, President Déby rejected the $2 million bribe offer. Ho subsequently drafted a letter to President Déby claiming that the cash had been intended as a donation to Chad. Ultimately, Ho and CEFC China did not obtain the unfair advantage that they had sought through the bribe offer, and by mid-2015, Ho had turned his attention to a different "gateway to Africa": Uganda.

The Uganda Scheme

According to the evidence presented at trial, the Uganda Scheme began around the same time as the Chad Scheme, when Ho was in New York, New York for the annual UN General Assembly. Ho met with Sam Kutesa, who had recently begun his term as the 69th President of the UN General Assembly ("PGA"). Ho, purporting to act on behalf of CEFC NGO, met with Kutesa and began to cultivate a relationship with him. During the year that Kutesa served as PGA, Ho and Kutesa discussed a "strategic partnership" between Uganda and CEFC China for various business ventures, to be formed once Kutesa completed his term as PGA and returned to Uganda.

In or about February 2016 – after Kutesa had returned to Uganda and resumed his role as Foreign Minister, and Yoweri Museveni (Kutesa's relative) had been reelected as the President of Uganda – Kutesa solicited a payment from Ho, purportedly for a charitable foundation that Kutesa wished to launch. Ho agreed to provide the requested payment, but simultaneously requested, on behalf of CEFC China, an invitation to Museveni's inauguration, business meetings with President Museveni and other high-level Ugandan officials, and a list of specific business projects in Uganda that CEFC China could participate in.

In May 2016, Ho and CEFC China executives traveled to Uganda. Prior to departing, Ho caused the CEFC NGO to wire $500,000 to the account provided by Kutesa in the name of the so-called "foundation," which wire was transmitted through banks in New York, New York. Ho also advised his boss, the Chairman of CEFC China, to provide $500,000 in cash to President Museveni, ostensibly as a campaign donation, even though Museveni had already been reelected. Ho intended these payments as bribes to influence Kutesa and Museveni to use their official power to steer business advantages to CEFC China.

Ho and CEFC China executives attended President Museveni's inauguration and obtained business meetings in Uganda with President Museveni and top Ugandan officials, including at the Department of Energy and Mineral Resources. After the trip, Ho requested that Kutesa and Museveni assist CEFC China in acquiring a Ugandan bank, as an initial step before pursuing additional ventures in Uganda. Ho also explicitly offered to "partner" with Kutesa and Museveni and/or their "family businesses," making clear that both officials would share in CEFC China's future profits. In exchange for the bribes offered and paid by Ho, Kutesa thereafter steered a bank acquisition opportunity to CEFC China.

This case was investigated by the FBI and IRS-CI. U.S. Immigration and Customs Enforcement's Homeland Security Investigations and the Department of Justice, Criminal Division's Office of International Affairs provided assistance.

Trial Attorney Paul A. Hayden of the Criminal Division's Fraud Section, FCPA Unit and Assistant U.S. Attorneys Douglas S. Zolkind, Daniel C. Richenthal and Catherine E. Ghosh of the U.S. Attorney's Office for Southern District of New York's Public Corruption Unit and the Criminal Division's Fraud Section are prosecuting the case.

The Fraud Section is responsible for investigating and prosecuting all FCPA matters. Additional information about the Justice Department's FCPA enforcement efforts can be found at www.justice.gov/criminal/fraud/fcpa.

Thursday, November 1, 2018

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

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. Attorney General Jeff Sessions, FBI Director Christopher Wray, Assistant Attorney General for National Security John Demers, Assistant Attorney General for the Criminal Division Brian A. Benczkowski, United States Attorney Alex G. Tse of the Northern District of California, and FBI Special Agent in Charge for the San Francisco Field Office John F. Bennett made the announcement.

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. The indictment was filed on September 27, 2018, and unsealed today. The civil lawsuit was filed today.

"I am announcing that a grand jury in San Francisco has returned a multi-defendant indictment alleging economic espionage on the part of a state-owned Chinese company, a Taiwanese company, and three Taiwan individuals for an alleged scheme to steal trade secrets from Micron, an Idaho-based semi-conductor company," said Attorney General Sessions. "The worldwide supply for DRAM is worth nearly $50 billion; Micron controls about 20 to 25 percent of the dynamic random access memory industry—a technology not possessed by the Chinese until very recently. As this and other recent cases have shown, Chinese economic espionage against the United States has been increasing—and it has been increasing rapidly. I am here to say that enough is enough. With integrity and professionalism, the Department of Justice will aggressively prosecute such illegal activity."

"The theft of intellectual property is not only unfair, but stifles technological innovation by disincentivizing investment in long-term research and development," said U.S. Attorney Alex Tse. "The theft of intellectual property on a continuing basis by nation-state actors is an even more damaging affront to the rule of law. We in the Northern District of California, one of the world's great centers of intellectual property development, will continue to lead the fight to

protect U.S. innovation from criminal misappropriation, whether motivated by personal greed or national economic ambition."

"No country presents a broader, more severe threat to our ideas, our innovation, and our economic security than China," said FBI Director Christopher Wray. "The Chinese government is determined to acquire American technology, and they're willing use a variety of means to do that – from foreign investments, corporate acquisitions, and cyber intrusions to obtaining the services of current or former company employees to get inside information. If China acquires an American company's most important technology – the very technology that makes it the leader in a field – that company will suffer severe losses, and our national security could even be impacted. We are committed to continuing to work closely with our federal, state, local, and private sector partners to counter this threat from China."

According to the indictment, the defendants were engaged in a conspiracy to steal the trade secrets of Micron Technology, Inc. (Micron), a leader in the global semiconductor industry specializing in the advanced research, development, and manufacturing of memory products, including dynamic random-access memory (DRAM). DRAM is a leading-edge memory storage device used in computer electronics. Micron is the only United States-based company that manufactures DRAM. According to the indictment, Micron maintains a significant competitive advantage in this field due in large part from its intellectual property, including its trade secrets that include detailed, confidential information pertaining to the design, development, and manufacturing of advanced DRAM products.

Prior to the events described in the indictment, the PRC did not possess DRAM technology, and the Central Government and State Council of the PRC publicly identified the development of DRAM and other microelectronics technology as a national economic priority. The criminal defendants are United Microelectronics Corporation ("UMC"), a Taiwan semiconductor foundry; Fujian Jinhua Integrated Circuit, Co., Ltd. ("Jinhua'"), a state-owned enterprise of the PRC; and three Taiwan nationals: Chen Zhengkun, a.k.a. Stephen Chen, age 55; He Jianting, a.k.a. J.T. Ho, age 42; and Wang Yungming, a.k.a. Kenny Wang, age 44. UMC is a publicly listed semiconductor foundry company traded on the New York Stock Exchange; is headquartered in Taiwan; and has offices worldwide, including in Sunnyvale, California. UMC mass produces integrated-circuit logic products based on designs and technology developed and provided by its customers. Jinhua is a state-owned enterprise of the PRC, funded entirely by the Chinese government, and established in February 2016 for the sole purpose of designing, developing, and manufacturing DRAM.

According to the indictment, Chen was a General Manager and Chairman of an electronics corporation that Micron acquired in 2013. Chen then became the president of a Micron subsidiary in Taiwan, Micron Memory Taiwan ("MMT"), responsible for manufacturing at least one of Micron's DRAM chips. Chen resigned from MMT in July 2015 and began working at UMC almost immediately. While at UMC, Chen arranged a cooperation agreement between UMC and Fujian Jinhua whereby, with funding from Fujian Jinhua, UMC would transfer DRAM technology to Fujian Jinhua to mass-produce. The technology would be jointly shared by both UMC and Fujian Jinhua. Chen later became the President of Jinhua and was put in charge of its DRAM production facility.

While at UMC, Chen recruited numerous MMT employees, including Ho and Wang, to join him at UMC. Prior to leaving MMT, Ho and Wang both stole and brought to UMC several

Micron trade secrets related to the design and manufacture of DRAM. Wang downloaded over 900 Micron confidential and proprietary files before he left MMT and stored them on USB external hard drives or in personal cloud storage, from where he could access the technology while working at UMC.

An indictment merely alleges that crimes have been committed, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt. If convicted, the individual defendants face a maximum sentence of 15 years imprisonment and a $5,000,000 fine for economic espionage charges, and 10 years imprisonment for theft of trade secrets charges. If convicted, each company faces forfeiture and a maximum fine of more than $20 billion. However, any sentence following conviction would be imposed by the court only after consideration of the U.S. Sentencing Guidelines and the federal statute governing the imposition of a sentence, 18 U.S.C. § 3553.

Tuesday, October 30 2018

Chinese Intelligence Officers And Their Recruited Hackers And Insiders Conspired To Steal Sensitive Commercial Aviation And Technological Data For Years

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.

The charged intelligence officers, Zha Rong and Chai Meng, and other co-conspirators, worked for the Jiangsu Province Ministry of State Security ("JSSD"), headquartered in Nanjing, which is a provincial foreign intelligence arm of the People's Republic of China's Ministry of State Security (MSS). The MSS, and by extension the JSSD, is primarily responsible for domestic counter-intelligence, non-military foreign intelligence, and aspects of political and domestic security.

From at least January 2010 to May 2015, JSSD intelligence officers and their team of hackers, including Zhang Zhang-Gui, Liu Chunliang, Gao Hong Kun, Zhuang Xiaowei, and Ma Zhiqi, focused on the theft of technology underlying a turbofan engine used in U.S. and European commercial airliners. This engine was being developed through a partnership between a French aerospace manufacturer with an office in Suzhou, Jiangsu province, China, and a company based in the United States. Members of the conspiracy, assisted and enabled by JSSD-recruited insiders Gu Gen and Tian Xi, hacked the French aerospace manufacturer. The hackers also conducted intrusions into other companies that manufactured parts for the turbofan jet engine, including aerospace companies based in Arizona, Massachusetts and Oregon. At the time of the intrusions, a Chinese state-owned aerospace company was working to develop a comparable engine for use in commercial aircraft manufactured in China and elsewhere.

Defendant Zhang Zhang-Gui is also charged, along with Chinese national Li Xiao, in a separate hacking conspiracy, which asserts that Zhang Zhang-Gui and Li Xiao leveraged the JSSD-directed conspiracy's intrusions, including the hack of a San Diego-based technology company, for their own criminal ends.

"For the third time since only September, the National Security Division, with its US Attorney partners, has brought charges against Chinese intelligence officers from the JSSD and those working at their direction and control for stealing American intellectual property," said John C. Demers, Assistant Attorney General for National Security. "This is just the beginning. Together with our federal partners, we will redouble our efforts to safeguard America's ingenuity and investment."

"This action is yet another example of criminal efforts by the MSS to facilitate the theft of private data for China's commercial gain," said U.S. Attorney Adam Braverman. "The concerted effort to steal, rather than simply purchase, commercially available products should offend every company that invests talent, energy, and shareholder money into the development of products."

"The threat posed by Chinese government-sponsored hacking activity is real and relentless," said John Brown, FBI Special Agent in Charge of the San Diego Field Office. "Today, the Federal Bureau of Investigation, with the assistance of our private sector, international and U.S. government partners, is sending a strong message to the Chinese government and other foreign governments involved in hacking activities. We are working together to vigorously investigate and hold hackers accountable regardless of their attempts to hide their illicit activities and identities."

On October 10, the Department of Justice announced that a JSSD intelligence officer was extradited to the Southern District of Ohio, on charges that he attempted to steal trade secrets related to jet aircraft engines, and in September, in the Northern District of Illinois, a grand jury indicted a U.S. Army recruit who is accused of working as an agent of a JSSD intelligence officer, without notification to the Attorney General.

As the indictment in the Southern District of California describes in detail, China's JSSD intelligence officers and hackers working at their direction masterminded a series of intrusions in order to facilitate intrusions and steal non-public commercial and other data. The hackers used a range of techniques, including spear phishing, sowing multiple different strains of malware into company computer systems, using the victim companies' own websites as "watering holes" to compromise website visitors' computers, and domain hijacking through the compromise of domain registrars.

The first alleged hack began no later January 8, 2010, when members of the conspiracy infiltrated Capstone Turbine, a Los-Angeles-based gas turbine manufacturer, in order to steal data and use the Capstone Turbine website as a "watering hole."

China's intelligence service also sought, repeatedly, to hack into a San Diego-based technology company from at least August 7, 2012 through January 15, 2014, in order to similarly steal commercial information and use its website as a "watering hole."

Chinese actors used not only hacking methods to conduct computer intrusions and steal commercial information, they also coopted victim company employees. From at least November 2013 through February 2014, two Chinese nationals working at the direction of the JSSD, Tian Xi and Gu Gen, were employed in the French aerospace company's Suzhou office. On January 25, 2014, after receiving malware from an identified JSSD officer acting as his handler, Tian infected one of the French company's computers with malware at the JSSD officer's direction. One month later, on February 26, 2014, Gu, the French company's head of Information

Technology and Security in Suzhou, warned the conspirators when foreign law enforcement notified the company of the existence of malware on company systems. That same day, leveraging that tip-off, conspirators Chai Meng and Liu Chunliang tried to minimize JSSD's exposure by causing the deletion of the domain linking the malware to an account controlled by members of the conspiracy.

The group's hacking attempts continued through at least May of 2015, when an Oregon-based company, which, like many of the other targeted companies, built parts for the turbofan jet engine used in commercial airliners, identified and removed the conspiracy's malware from its computer systems.

Count Two of the indictment charges a separate conspiracy to hack computers in which Zhang Zhang-Gui, a defendant charged in Count One, supplied his co-defendant and friend, Li Xiao, with variants of the malware that had been developed and deployed by hackers working at the direction of the JSSD on the hack into Capstone Turbine. Using malware supplied by Zhang, as well as other malware, Li launched repeated intrusions that targeted a San Diego-based computer technology company for more than a year and a half. These intrusions caused thousands of dollars of damage to protected computers.

Count Three of the indictment charges Zhang Zhang-Gui with the substantive offense of computer hacking a San Diego technology company, which was one of the targets of the conspiracies alleged in Counts One and Two.

The charges contained in the indictment are merely accusations, and the defendants are presumed innocent unless and until proven guilty.

The FBI, led by the San Diego Field Office, conducted the investigation that resulted in charges announced today. This case is being prosecuted by Alexandra Foster and Sabrina Fève of the United States Attorney's Office for the Southern District of California and Jason McCullough of the National Security Division's Counterintelligence and Export Control Section. The Criminal Division's Office of International Affairs also provided assistance in this matter, and the Department appreciates the cooperation and assistance provided by France's General Directorate for Internal Security (DGSI) and the Cybercrime Section of the Paris Prosecutor's Office during the investigation of this matter.

Wednesday, October 10, 2018

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

A Chinese Ministry of State Security (MSS) operative, Yanjun Xu, aka Qu Hui, aka Zhang Hui, has been 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 yesterday.

The charges were announced today by Assistant Attorney General for National Security John C. Demers, U.S. Attorney for the Southern District of Ohio Benjamin C. Glassman, Assistant Director Bill Priestap of the FBI's Counterintelligence Division, and Special Agent in Charge Angela L. Byers of the FBI's Cincinnati Division.

"This indictment alleges that a Chinese intelligence officer sought to steal trade secrets and other sensitive information from an American company that leads the way in aerospace,"

said Assistant Attorney General Demers. "This case is not an isolated incident. It is part of an overall economic policy of developing China at American expense. We cannot tolerate a nation's stealing our firepower and the fruits of our brainpower. We will not tolerate a nation that reaps what it does not sow."

"Innovation in aviation has been a hallmark of life and industry in the United States since the Wright brothers first designed gliders in Dayton more than a century ago," said U.S. Attorney Glassman. "U.S. aerospace companies invest decades of time and billions of dollars in research. This is the American way. In contrast, according to the indictment, a Chinese intelligence officer tried to acquire that same, hard-earned innovation through theft. This case shows that federal law enforcement authorities can not only detect and disrupt such espionage, but can also catch its perpetrators. The defendant will now face trial in federal court in Cincinnati."

"This unprecedented extradition of a Chinese intelligence officer exposes the Chinese government's direct oversight of economic espionage against the United States," said Assistant Director Priestap.

Yanjun 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.

Xu was arrested in Belgium on April 1, pursuant to a federal complaint, and then indicted by a federal grand jury in the Southern District of Ohio. The government unsealed the charges today, following his extradition to the United States. The four-count indictment charges Xu with conspiring and attempting to commit economic espionage and theft of trade secrets.

***

According to the indictment:

Beginning in at least December 2013 and continuing until his arrest, Xu targeted certain companies inside and outside the United States that are recognized as leaders in the aviation field. This included GE Aviation. He identified experts who worked for these companies and recruited them to travel to China, often initially under the guise of asking them to deliver a university presentation. Xu and others paid the experts' travel costs and provided stipends.

***

An indictment is merely a formal charge that a defendant has committed a violation of criminal law and is not evidence of guilt. Every defendant is presumed innocent until, and unless, proven guilty.

The maximum statutory penalty for conspiracy and attempt to commit economic espionage is 15 years of incarceration. The maximum for conspiracy and attempt to commit theft of trade secrets is 10 years. The charges also carry potential financial penalties. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, a defendant's sentence will be determined by the court based on the advisory Sentencing Guidelines and other statutory factors.

This investigation was conducted by the FBI's Cincinnati Division, and substantial support was provided by the FBI Legal Attaché's Office in Brussels. The Justice Department's

Office of International Affairs provided significant assistance in obtaining and coordinating the extradition of Xu, and Belgian authorities provided significant assistance in securing the arrest and facilitating the surrender of Xu from Belgium.

Assistant Attorney General Demers and U.S. Attorney Glassman commended the investigation of this case by the FBI and the assistance of the Belgian authorities in the arrest and extradition of Xu. Mr. Demers and Mr. Glassman also commended the cooperation of GE Aviation throughout this investigation. The cooperation and GE Aviation's internal controls protected GE Aviation's proprietary information.

The case is being prosecuted by Assistant U.S. Attorneys Timothy S. Mangan and Emily N. Glatfelter of the Southern District of Ohio, and Trial Attorneys Thea D. R. Kendler and Amy E. Larson of the National Security Division's Counterintelligence and Export Control Section.

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

Ji Chaoqun, 27, a Chinese citizen residing in Chicago, was arrested in Chicago today for allegedly acting within the United States as an illegal agent of the People's Republic of China.

The arrest and complaint were announced by Assistant Attorney General for National Security John C. Demers, U.S. Attorney John R. Lausch, Jr. for the Northern District of Illinois, and Special Agent in Charge Jeffrey S. Sallet of the FBI's Chicago field office.

Ji worked at the direction of a high-level intelligence officer in the Jiangsu Province Ministry of State Security, a provincial department of the Ministry of State Security for the People's Republic of China, according to a criminal complaint and affidavit filed in U.S. District Court in Chicago. Ji was tasked with providing the intelligence officer with biographical information on eight individuals for possible recruitment by the JSSD, the complaint states. The individuals included Chinese nationals who were working as engineers and scientists in the United States, some of whom were U.S. defense contractors, according to the complaint.

The complaint charges Ji 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 will make an initial court appearance today at 5:00 p.m. EDT (4:00 p.m. CDT) before U.S. Magistrate Judge Michael T. Mason in Courtroom 2266 of the Everett M. Dirksen U.S. Courthouse in Chicago.

According to the complaint, Ji was born in China and arrived in the United States in 2013 on an F1 Visa, for the purpose of studying electrical engineering at the Illinois Institute of Technology in Chicago. In 2016, Ji enlisted in the U.S. Army Reserves as an E4 Specialist under the Military Accessions Vital to the National Interest (MAVNI) program, which authorizes the U.S. Armed Forces to recruit certain legal aliens whose skills are considered vital to the national interest. In his application to participate in the MAVNI program, Ji specifically denied having had contact with a foreign government within the past seven years, the complaint states. In a subsequent interview with a U.S. Army officer, Ji again failed to disclose his relationship and contacts with the intelligence officer, the charge alleges.

A criminal complaint is merely an accusation. The defendant is presumed innocent unless and until proven guilty. The charge carries a maximum sentence of ten years in

prison. The statutory maximum penalty is prescribed by Congress and is provided here for informational purposes only, as any sentencing of the defendant will be determined by the judge.

The U.S. Army 902nd Military Intelligence Group provided valuable assistance. The government's case is represented by Assistant U.S. Attorney Shoba Pillay of the Northern District of Illinois and Senior Trial Attorney Heather Schmidt of the National Security Division's Counterintelligence and Export Control Section.

Friday, June 8, 2018

Jury Convicts Former CIA Officer of Espionage

Today, a federal jury convicted Kevin Patrick Mallory, 61, a former Central Intelligence Agency case officer of Leesburg, Virginia, on espionage charges related to his transmission of classified documents to an agent of the People's Republic of China.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney G. Zachary Terwilliger for the Eastern District of Virginia and Assistant Director in Charge Nancy McNamara of the FBI's Washington Field Office made the announcement after Senior U.S. District Judge T.S. Ellis III accepted the verdict.

"It is a sad day when an American citizen is convicted of spying on behalf of a foreign power," said Assistant Attorney General Demers. "This act of espionage was no isolated incident. The People's Republic of China has made a sophisticated and concerted effort to steal our nation's secrets. Today's conviction demonstrates that we remain vigilant against this threat and hold accountable all those who put the United States at risk through espionage."

"There are few crimes in this country more serious than espionage," said U.S. Attorney Terwilliger. "This office has a long history of holding those accountable who betray their country and try and profit off of classified information. This case should send a message to anyone considering violating the public's trust and compromising our national security by disclosing classified information. We will remain steadfast and dogged in pursuit of these challenging but critical national security cases."

"This trial highlights a serious threat to U.S. national security," said Assistant Director in Charge McNamara. "Foreign intelligence agents are targeting former U.S. Government security clearance holders in order to recruit them and steal our secrets. This case should send a message to foreign intelligence services and those caught up in their web: we are watching and we will investigate and prosecute those who willfully violate their obligations to protect national security secrets. I want to start by thanking the prosecutors of the U.S. Attorney's Office, the trial attorneys of the Justice Department and particularly the special agents, analysts and professional staff of the FBI's Washington Field Office for their hard work."

According to court records and evidence presented at trial, in March and April 2017, Mallory travelled to Shanghai and met with an individual, Michael Yang, whom he quickly concluded was working for the People's Republic of China Intelligence Service (PRCIS). During a voluntary interview with FBI agents on May 24, 2007, Mallory stated that Yang represented himself as working for a People's Republic of China think tank, however Mallory stated that he assessed Yang to be a Chinese Intelligence Officer.

Mallory, a U.S. citizen who speaks fluent Mandarin Chinese, told FBI agents he travelled to Shanghai in March and April to meet with Yang and Yang's boss. After Mallory consented to

a review of a covert communications (covcom) device he had been given by Yang in order to communicate covertly with Yang, FBI agents viewed a message from Mallory to Yang in which Mallory stated that he could come in the middle of June and he could bring the remainder of the documents with him at that time. Analysis of the device, which was a Samsung Galaxy smartphone, also revealed a handwritten index describing eight different documents later determined to be classified. Four of the eight documents listed in the index were found stored on the device, with three being confirmed as containing classified information pertaining to the same U.S. government agency. One of those documents was classified TOP SECRET, while the remaining two documents were classified SECRET. FBI analysts were able to determine that Mallory had completed all of the steps necessary to securely transmit at least four documents via the covcom device, one of which contained unique identifiers for human sources who had helped the U.S. government.

Evidence presented at trial included surveillance video from a FedEx store in Leesburg where Mallory could be seen scanning the eight classified documents and a handwritten table of contents onto a micro SD card. Though Mallory shredded the paper copies of the eight documents, an SD card containing those documents and table of contents was later found carefully concealed in his house when it was searched on June 22, 2017, the date of his arrest. A recording was played at trial from June 24, 2017, where Mallory could be heard on a call from the jail calling his family to ask them to search for the SD card.

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. As required for his various government positions, Mallory obtained a Top Secret security clearance, which was active during various assignments during his career. Mallory's security clearance was terminated in October 2012 when he left government service.

Mallory was convicted of conspiracy to deliver, attempted delivery, delivery of defense information to aid a foreign government, and making material false statements. He faces a maximum penalty of life in prison when sentenced on Sept. 21. The statutory maximum penalty is prescribed by Congress and is provided here for informational purposes only, as any sentencing of the defendant will be determined by the judge.

Assistant U.S. Attorneys John T. Gibbs and Colleen E. Garcia of the Eastern District of Virginia, and Trial Attorney Jennifer Kennedy Gellie of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

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

Two businessmen, including one who is a Chinese national, have been indicted on charges alleging that 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.

The charges were announced today by Assistant Attorney General for National Security John C. Demers, U.S. Attorney for the District of Columbia Jessie K. Liu, Assistant Director Bill

Priestap of the FBI's Counterintelligence Division, Special Agent in Charge Perrye K. Turner of the FBI's Houston Field Office, and Chief Don Fort of the Internal Revenue Service's Criminal Investigation (IRS-CI).

Shan Shi, 53, a U.S. citizen from Houston, Texas, and Gang Liu, 32, a Chinese national, were among six individuals named in a superseding indictment returned on April 26, 2018, in the U.S. District Court for the District of Columbia. All six individuals initially were indicted in June 2017 on a charge of conspiracy to commit theft of trade secrets. The superseding indictment includes that charge and adds the conspiracy to commit economic espionage count against Shi and Liu, as well as a federal money laundering conspiracy count against Shi. CBM-Future New Material Science and Technology Co. Ltd. (CBMF), a Chinese company based in Taizhou, and its Houston-based subsidiary, CBM International, Inc. (CBMI), have also been indicted on all three charges.

The other defendants include Uka Kalu Uche, 36, a U.S. citizen from Spring, Texas; Samuel Abotar Ogoe, 75, a U.S. citizen from Missouri City, Texas; Kui Bo, 41, a Canadian citizen who had been residing in the Dallas area; and Hui Huang, 33, a Chinese national. All of the defendants pled not guilty last year to the charges in the original indictment, with the exception of Huang, who has not been apprehended and is believed to remain at large in China.

A seventh defendant previously pled guilty in December 2017 to a charge of conspiracy to commit theft of trade secrets.

"The superseding indictment in this case demonstrates that we will vigorously enforce laws meant to protect against economic espionage and related offenses," said U.S. Attorney Liu. "The charges also reflect the tireless dedication of the FBI, Commerce Department's BIS, IRS, and other law enforcement organizations to prosecuting theft of intellectual property."

"The ongoing theft of American technology is a severe threat to our national security, and this is doubly true for technology with direct military applications. As this situation demonstrates, the FBI remains committed to working with its partners to combat this threat," said FBI Assistant Director for Counterintelligence Priestap.

"This indictment is a good example of the community, industry, and law enforcement working together," said FBI Special Agent in Charge Turner. "Economic espionage is a growing threat that costs the U.S. economy billions of dollars and puts our national security at risk. The FBI will continue to work with its partners to bring perpetrators of economic espionage to justice."

"This superseding indictment alleges a vast criminal conspiracy involving everything from trade secret theft to money laundering and other financial crimes," said IRS Criminal Investigation Chief Fort. "By unraveling this scheme, we were able to hold those accountable who would profit from such a scheme while sending a message to others who would commit similar crimes in the future that they, too, will be brought to justice."

According to the indictment, China has promoted military, social, and economic development initiatives with a goal of making the country a marine power and has prioritized the development of engineered components of deepwater buoyancy materials. The charges in the indictment involve the development of syntactic foam, a strong, lightweight material that can be tailored for commercial and military uses, including oil exploration, aerospace and stealth technologies, and underwater vehicles, such as submarines.

According to the indictment, from at least 2013 through May 2017, Shi operated on behalf of CBMF, which intended to create a facility in China to sell syntactic foam. CBMF received research funds from state funding in China and was part of a collaborative innovation center with Chinese government entities.

The indictment alleges that Shi and Liu conspired with the other defendants to steal trade secrets from a global engineering firm, referred to in the indictment as "Company A," that is a producer in the global syntactic foam market.

In March 2014, according to the indictment, Shi incorporated CBMI, which was owned and funded by CBMF, in Houston. The indictment alleges that CBMF employees wired approximately $3.1 million to CBMI between June 2014 and May 2017.

According to the indictment, Shi and others recruited and hired current and former employees of "Company A" in Houston, including Liu, for the purpose of aiding CBMF's capability to make syntactic foam. Liu previously worked for "Company A" as a material development engineer and had access to proprietary and trade secret data. He and others are accused of passing along those trade secrets. According to the indictment, the technology was ultimately destined for China, to benefit the government and other state-owned enterprises.

An indictment is merely a formal charge that a defendant has committed a violation of criminal law and is not evidence of guilt. Every defendant is presumed innocent until, and unless, proven guilty.

The maximum statutory penalty for conspiracy to commit economic espionage is 15 years of incarceration. The maximum for conspiracy to commit theft of trade secrets is 10 years, and the maximum for conspiracy to commit money laundering is 20 years. The charges also carry potential financial penalties. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, a defendant's sentence will be determined by the court based on the advisory Sentencing Guidelines and other statutory factors.

The case is being investigated by the FBI's Houston Field Office, Commerce's BIS Office of Export Enforcement, and the IRS-CI.

The case is being prosecuted by Assistant U.S. Attorneys Jeffrey Pearlman, Zia Faruqui, and Michael Romano of the District of Columbia, and Trial Attorney David Recker of the National Security Division's Counterintelligence and Export Control Section.

Wednesday, April 4, 2018

Chinese Scientist Sentenced to Prison in Theft of Engineered Rice

A Chinese scientist 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.

Acting Assistant Attorney General John P. Cronan of the Justice Department's Criminal Division, Assistant Attorney General John C. Demers of the Justice Department's National Security Division and U.S. Attorney Stephen R. McAllister of the District of Kansas made the announcement.

Weiqiang Zhang, 51, a Chinese national, and U.S. legal permanent resident residing in Manhattan, Kansas, was sentenced by U.S. District Court Judge Carlos Murguia in the District of

Kansas. Zhang was convicted on Feb. 15, 2017 of one count of conspiracy to steal trade secrets, one count of conspiracy to commit interstate transportation of stolen property and one count of interstate transportation of stolen property.

Evidence at trial established that Zhang worked as a rice breeder for Ventria Bioscience in Junction City, Kansas. Ventria develops genetically programmed rice to express recombinant human proteins, which are then extracted for use in the therapeutic and medical fields. Zhang has a master's degree in agriculture from Shengyang Agricultural University in China and a doctorate from Louisiana State University.

According to trial evidence, Zhang acquired without authorization hundreds of rice seeds produced by Ventria and stored them at his residence in Manhattan. The rice seeds have a wide variety of health research applications and were developed to produce either human serum albumin, contained in blood, or lactoferrin, an iron-binding protein found, for example, in human milk. Ventria spent millions of dollars and years of research developing its seeds and cost-effective methods to extract the proteins, which are used to develop lifesaving products for global markets. Ventria used locked doors with magnetic card readers to restrict access to the temperature-controlled environment where the seeds were stored and processed.

Trial evidence demonstrated that in the summer of 2013, personnel from a crop research institute in China visited Zhang at his home in Manhattan. Zhang drove the visitors to tour facilities in Iowa, Missouri and Ohio. On Aug. 7, 2013, U.S. Customs and Border Protection officers found seeds belonging to Ventria in the luggage of Zhang's visitors as they prepared to leave the United States for China.

"Weiqiang Zhang betrayed his employer by unlawfully providing its proprietary rice seeds to representatives of a Chinese crop institute," said Acting Assistant Attorney General Cronan. "Today's sentence demonstrates the significant consequences awaiting those who would steal trade secrets from American companies. The Criminal Division and its law enforcement partners will continue to work closely with companies like Ventria to protect American intellectual property—which is essential to our economy and way of life—against all threats both foreign and domestic."

"Cross-border intellectual property theft not only hurts victim companies, it also threatens our national security," said Assistant Attorney General Demers. "FBI's vigilance stopped Ventria's intellectual property from leaving our country in the nick of time, but it was Ventria's cooperation that allowed us to hold Zhang accountable for his crimes."

"Ventria invested years of research and tens of millions of dollars to create a new and beneficial product," said U.S. Attorney McAllister. "It is vital that we protect such intellectual property from theft and exploitation by foreign interests. We all benefit when American companies continue to drive socially valuable advancements in food, medicine and technology."

The FBI's Little Rock, Arkansas, Field Office and Kansas City, Missouri, Field Office, U.S. Customs and Border Protection and the U.S. Attorney's Office for the Eastern District of Arkansas investigated the case. Trial Attorney Matt Walczewski of the National Security Division, Trial Attorneys Brian Resler and Evan Williams of the Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorney Scott Rask of the District of Kansas prosecuted the case.

Friday, January 19, 2018

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

Federal authorities this morning arrested two local men on federal charges that allege a scheme to illegally obtain technology and integrated circuits with military applications that were exported to a Chinese company without the required export license.

Yi-Chi Shih, 62, an electrical engineer who is a part-time Los Angeles resident, and Kiet Ahn Mai, 63, of Pasadena, were arrested this morning without incident by federal agents.

Shih and Mai, who previously worked together at two different companies, are named in a criminal complaint unsealed this morning that charges them with conspiracy. Shih is also charged with violating the International Emergency Economic Powers Act (IEEPA), a federal law that makes illegal, among other things, certain unauthorized exports.

The 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.

According to the affidavit in support of the criminal complaint, Shih and Mai executed a scheme to defraud the U.S. company out of its proprietary, export-controlled items, including technology associated with its design services for MMICs. As part of the scheme, Shih and Mai accessed the victim company's computer systems via its web portal after Mai obtained that access by posing as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih and Mail allegedly concealed Shih's true intent to transfer the U.S. company's technology and products to the People's Republic of China.

"This case outlines a scheme to secure proprietary technology, some of which was allegedly sent to China, where it could be used to provide companies there with significant advantages that would compromise U.S. business interests," said United States Attorney Nicola T. Hanna. "The very sensitive information would also benefit foreign adversaries who could use the technology to further or develop military applications that would be detrimental to our national security."

"According to the complaint, the defendants allegedly schemed to illegally export semiconductors having military and civilian applications to a Chinese company," said Acting Assistant Attorney General Boente. "Protecting this type of technology and preventing its illegal acquisition by our adversaries remains a key priority in preserving our national security."

The victim company's proprietary semiconductor technology has a number of commercial and military applications, and its customers include the Air Force, Navy and the Defense Advanced Research Projects Agency. MMICs are used in electronic warfare, electronic warfare countermeasures and radar applications.

"The FBI, working jointly with our law enforcement partners, remains committed to bringing to justice those who seek to illegally export some of our nation's most sensitive technologies to the detriment of our national security and hard-working United States companies," said Paul Delacourt, Assistant Director in Charge of the FBI's Los Angeles Field Office. "Rest assured, the FBI will continue to diligently pursue any and all leads that involve the

illegal exportation of U.S. technology which will cause harm to our long-term national security interests."

The computer chips at the heart of this case allegedly were shipped to Chengdu GaStone Technology Company (CGTC), a Chinese company that established a MMIC manufacturing facility in Chengdu. Shih was the president of CGTC, which in 2014 was placed on the Commerce Department's Entity List, according to the affidavit, "due to its involvement in activities contrary to the national security and foreign policy interest of the United States – specifically, that it had been involved in the illicit procurement of commodities and technologies for unauthorized military end use in China." Because it was on the Entity List, a license from the Commerce Department was required to export U.S.-origin MMICs to CGTC, and there was a "presumption of denial" of a license.

The complaint outlines a scheme in which Shih used a Los Angeles-based company he controlled – Pullman Lane Productions, LLC – to funnel funds provided by Chinese entities to finance the manufacturing of MMICs by the victim company. The complaint affidavit alleges that Pullman Lane received financing from a Beijing-based company that was placed on the Entity List the same day as CGTC "on the basis of its involvement in activities contrary to the national security and foreign policy interests of the United States."

Mai acted as the middleman by using his Los Angeles company – MicroEx Engineering – to pose as a legitimate domestic customer that ordered and paid for the manufacturing of MMICs that Shih illegally exported to CGTC in China, according to the complaint. It is the export of the MMICs that forms the basis of the IEEPA violation alleged against Shih. The specific exported MMICs also required a license from the Commerce Department before being exported to China, and a license was never sought or obtained for this export.

"Today's actions serve as a reminder that the government will hold individuals accountable who fraudulently procure and export unlawfully protected United States technology and attempt to conceal their criminal activity through international money laundering," stated Special Agent in Charge R. Damon Rowe with IRS Criminal Investigation. "The IRS plays an important role in tracing illicit funds through both domestic and international financial intuitions. The IRS is proud to partner with the FBI and Department of Commerce and share its world-renowned financial investigative expertise in this investigation."

"Today's arrests demonstrate the Office of Export Enforcement's strong commitment to enforcing our nation's export control and public safety laws," said Richard Weir, Special Agent in Charge of the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement, Los Angeles Field Office. "We will continue to work with our law enforcement partners to identify, deter, and keep the most sensitive U.S. origin goods and technology out of the most dangerous hands."

Shih and Mai are expected to make their first court appearances this afternoon in United States District Court in downtown Los Angeles.

A criminal complaint contains allegations that a defendant has committed a crime. Every defendant is presumed to be innocent until and unless proven guilty in court.

If they were to be convicted of the charges in the criminal complaint, Mai would face a statutory maximum sentence of five years in federal prison, and Shih could be sentenced to as much as 25 years in prison.

This case is being investigated by the Federal Bureau of Investigation; the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and IRS Criminal Investigation.

The case against Shih and Mai is being prosecuted by Assistant United States Attorneys Judith A. Heinz, Melanie Sartoris and Khaldoun Shobaki of the National Security Division, and Trial Attorney Matthew Walczewski of the Department of Justice's National Security Division.

Thursday, January 18, 2018

Chinese National Sentenced for Economic Espionage and Theft of a Trade Secret From U.S. Company

Xu Jiaqiang, 31, formerly of Beijing, China, was sentenced yesterday 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 the intent to benefit the National Health and Family Planning Commission of the People's Republic of China. Xu previously pleaded guilty to all six counts with which he was charged.

Acting Assistant Attorney General for National Security Dana J. Boente and U.S. Attorney Geoffrey S. Berman for the Southern District of New York made the announcement. The sentence was imposed by U.S. District Judge Kenneth M. Karas in White Plains, New York federal court.

"Xu, a Chinese national, is being held accountable for engaging in economic espionage against an American company," said Acting Assistant Attorney General Boente. "Xu not only stole high tech trade secrets from his U.S. employer – a federal crime – he did so both for his own profit and intending to benefit the Chinese government. Xu's sentence clearly demonstrates that the National Security Division will not hesitate to pursue and prosecute those who steal from American businesses. I thank the many people who worked hard to bring this result."

"As he previously admitted in federal court, Xu Jiaqiang stole high-tech trade secrets from a U.S. employer, intending to benefit the Chinese government," said U.S. Attorney Berman. "The laws governing economic espionage and trade secrets exist, in part, to protect the sanctity of American ingenuity and property. Xu's prison sentence should be a red flag for anyone attempting to illegally peddle American expertize and intellectual property to foreign bidders."

According to the allegations contained in the Complaint and the Superseding Indictment filed against Xu, as well as statements made in related court filings and proceedings:

From November 2010 to May 2014, Xu worked as a developer for a particular U.S. company (the Victim Company). As a developer, Xu enjoyed access to certain proprietary software (the Proprietary Software), as well as that software's underlying source code (the Proprietary Source Code). The Proprietary Software is a clustered file system developed and marketed by the Victim Company in the United States and other countries. A clustered file system facilitates faster computer performance by coordinating work among multiple servers. The Victim Company takes significant precautions to protect the Proprietary Source Code as a trade secret. Among other things, the Proprietary Source Code is stored behind a company firewall and can be accessed only by a small subset of the Victim Company's employees. Before receiving Proprietary Source Code access, Victim Company employees must first request and receive approval from a particular Victim Company official. Victim Company

employees must also agree in writing at both the outset and the conclusion of their employment that they will maintain the confidentiality of any proprietary information. The Victim Company takes these and other precautions in part because the Proprietary Software and the Proprietary Source Code are economically valuable, which value depends in part on the Proprietary Source Code's secrecy.

In May 2014, Xu voluntarily resigned from the Victim Company. Xu subsequently communicated with one undercover law enforcement officer (UC-1), who posed as a financial investor aiming to start a large-data storage technology company, and another undercover law enforcement officer (UC-2), who posed as a project manager, working for UC-1. In these communications, Xu discussed his past experience with the Victim Company and indicated that he had experience with the Proprietary Software and the Proprietary Source Code. On March 6, 2015, Xu sent UC-1 and UC-2 a code, which Xu stated was a sample of Xu's prior work with the Victim Company. A Victim Company employee (Employee-1) later confirmed that the code sent by Xu included proprietary Victim Company material that related to the Proprietary Source Code.

Xu subsequently informed UC-2 that Xu was willing to consider providing UC-2's company with the Proprietary Source Code as a platform for UC-2's company to facilitate the development of its own data storage system. Xu informed UC-2 that if UC-2 set up several computers as a small network, then Xu would remotely install the Proprietary Software so that UC-1 and UC-2 could test it and confirm its functionality.

In or around early August 2015, the FBI arranged for a computer network to be set up, consistent with Xu's specifications. Files were then remotely uploaded to the FBI-arranged computer network (the Xu Upload). Thereafter, on or about Aug. 26, 2015, Xu and UC-2 confirmed that UC-2 had received the Xu Upload. In September 2015, the FBI made the Xu Upload available to a Victim Company employee who has expertise regarding the Proprietary Software and the Proprietary Source Code (Employee-2). Based on Employee-2's analysis of technical features of the Xu Upload, it appeared to Employee-2 that the Xu Upload contained a functioning copy of the Proprietary Software. It further appeared to Employee-2 that the Xu Upload had been built by someone with access to the Proprietary Source Code who was not working within the Victim Company or otherwise at the Victim Company's direction.

On Dec. 7, 2015, Xu met with UC-2 at a hotel in White Plains, New York (the Hotel). Xu stated, in sum and substance, that Xu had used the Proprietary Source Code to make software to sell to customers, that Xu knew the Proprietary Source Code to be the product of decades of work on the part of the Victim Company, and that Xu had used the Proprietary Source Code to build a copy of the Proprietary Software, which Xu had uploaded and installed on the UC Network (i.e., the Xu Upload). Xu also indicated that Xu knew the copy of the Proprietary Software that Xu had installed on the UC Network contained information identifying the Proprietary Software as the Victim Company's property, which could reveal the fact that the Proprietary Software had been built with the Proprietary Source Code without the Victim Company's authorization. Xu told UC-2 that Xu could take steps to prevent detection of the Proprietary Software's origins – i.e., that it had been built with stolen Proprietary Source Code – including writing computer scripts that would modify the Proprietary Source Code to conceal its origins.

Later on Dec. 7, 2015, Xu met with UC-1 and UC-2 at the Hotel. During that meeting, Xu showed UC-2 a copy of what Xu represented to be the Proprietary Source Code on Xu's laptop. Xu noted to UC-2 a portion of the code that indicated it originated with the Victim Company as well as the date on which it had been copyrighted. Xu also stated that Xu had previously modified the Proprietary Source Code's command interface to conceal the fact that the Proprietary Source Code originated with the Victim Company and identified multiple specific customers to whom Xu had previously provided the Proprietary Software using Xu's stolen copy of the Proprietary Source Code.

* * *

Mr. Boente and Mr. Berman praised the FBI's outstanding investigative efforts. Mr. Berman also thanked the U.S. Department of Justice's National Security Division.

Assistant U.S. Attorneys Benjamin Allee and Ilan Graff of the Southern District of New York, with assistance from Trial Attorney David Aaron of the National Security Division's Counterintelligence and Export Control Section, are in charge of the prosecution.