# Year in Review for China-Related Cases

**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.