JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Monday, December 19, 2016

Chinese National Admits to Stealing Sensitive Military Program Documents From United Technologies

Yu Long, 38, a citizen of China and lawful permanent resident of the U.S., waived his right to be indicted and pleaded guilty today in New Haven federal court in Connecticut, to charges related to his theft of numerous sensitive military program documents from United Technologies and transporting them to China.

Long pleaded guilty to one count of conspiracy to engage in the theft of trade secrets knowing that the offense would benefit a foreign government, foreign instrumentality or foreign agent, an offense that carries a maximum term of imprisonment of 15 years. He also pleaded guilty to one count of unlawful export and attempted export of defense articles from the U.S. in violation of the Arms Export Control Act, an offense that carries a maximum term of imprisonment of 20 years. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, the sentencing of the defendant will be determined by the court based on the advisory Sentencing Guidelines and other statutory factors.

The announcement was made by Acting Assistant Attorney General for National Security Mary B. McCord, U.S. Attorney Deirdre M. Daly for the District of Connecticut, Special Agent in Charge Matthew Etre of the FBI's Homeland Security Investigations (HSI) in Boston, Massachusetts, Special Agent in Charge Craig W. Rupert of the Defense Criminal Investigative Service (DCIS) Northeast Field Office, Special Agent in Charge Patricia M. Ferrick of the FBI's New Haven Division and Special Agent in Charge Danielle Angley with the Air Force Office of Special Investigations (AFOSI).

"Long admitted to stealing and exploiting highly sensitive military technology and documents, knowing his theft would benefit China's defense industry and deliberately contravene the embargo on U.S. Munitions List technology the United States has imposed on China," said Acting Assistant Attorney General McCord. "Export laws exist as an important part of our national security framework and disrupting and prosecuting this kind of economic espionage is one of the National Security Division's highest priorities."

"In an effort to further his own career, this defendant stole an extraordinary amount of proprietary military program information from United Technologies and transported much of that stolen information to China," said U.S. Attorney Daly. "His actions, which he knew would benefit China, not only violated his employment agreement and damaged the company, but have threatened our country's national security interests. U.S. companies continue to be targeted by those who seek to steal intellectual property, trade secrets and advanced defense technology – whether through a computer hack or cyber intrusion, or through a rogue employee. Working closely with our nation's defense contractors, we will relentlessly investigate and prosecute those who steal, or attempt to steal, trade secrets and sensitive military information, whether for their own personal gain or for the benefit of foreign actors."

"These sophisticated technologies are highly sought after by our adversaries," said Special Agent in Charge Etre. "They were developed to give the United States and its allies a distinct military advantage, which is why HSI and our law enforcement partners will continue to aggressively target the individuals who steal the ideas of others and sell these items."

"Today's plea demonstrates the commitment of the Defense Criminal Investigative Service and our federal law enforcement partners to identifying those who illegally export sensitive defense information to adversarial Foreign governments," said Special Agent in Charge Rupert. "DCIS will continue to safeguard sensitive technology and to shield America's investment in national defense by disrupting efforts of groups and individuals who try to illegally acquire our national security assets."

“This case highlights the complexity in which the FBI and law enforcement are being challenged to keep the integrity of our industry intellectual property intact,” said Special Agent in Charge Ferrick. “Investigating criminal activity of this nature will continue to be a priority.”

“This case was enabled by the outstanding teamwork of the FBI, DCIS, HSI, AFOSI and the U.S. Attorney's office,” said, Special Agent in Charge Angley. “In addition, it demonstrates the focus of law enforcement agencies to protect our nation's critical resources.”

According to court documents and statements made in court, from approximately May 2008 to May 2014, Long worked as a Senior Engineer/Scientist at United Technologies Research Center (UTRC) in Connecticut. Long’s employment at UTRC included work on F119 and F135 engines. The F119 engine is employed by the U.S. Air Force F-22 Raptor fighter aircraft, and the F135 engine is employed by the U.S. Air Force F-35 Lightning II fighter aircraft.

Beginning in 2013, Long expressed his intent to individuals outside UTRC to return to China to work on research projects at certain state-run universities in China using knowledge and materials he had acquired while employed at the UTRC. To that end, Long interacted with several state-run institutions in China, including the Chinese Academy of Science (CAS) and the Shenyang Institute of Automation (SIA), a state-run university in China affiliated with CAS.

During 2013 and 2014, Long was recruited by SIA and other state-run universities, during which he leveraged information that he had obtained while working at UTRC to seek employment in China, culminating in his travel to China in the possession of voluminous documents and data containing highly sensitive intellectual property, trade secrets and export controlled technology, which he had unlawfully stolen from UTRC.

In December 2013, after Long agreed in principle to join SIA, an SIA-CAS Director and an SIA-CAS Recruiter asked Long to provide documents from his work at UTRC and examples of projects on which he had worked to substantiate the claims Long made in his application, and interview with SIA. Long agreed.

On Dec. 24, 2013, Long emailed several documents to the SIA-CAS Director, including a document that contained the cover page of an export controlled UTRC presentation on Distortion Modeling dated Sept. 30, 2011.

While negotiating with SIA, Long also continued to explore other opportunities at other state-run institutions in China. In one email, Long stated: “I have made my mind to return to China, so have prepared a research plan based on my industry experience and current projects.” In the research plan, Long stated: “In the past five years, I have been working with Pratt Whitney, also other UTC business units, like UTAS (including Hamilton Sundstrand and Goodrich), Sikorsky, CCS (including Carrier and Fire & Security), and Otis. These unique working experiences have provided me a great starting point to perform R&D and further spin off business in China. I believe my efforts will help China to mature its own aircraft engines.”

On May 30, 2014, Long left UTRC. In June 2014, Long traveled to China and began working for SIA. Beginning in July 2014, digital evidence and forensic analysis indicated that Long brought with him and accessed in China a UTRC external hard drive that had been issued to him and that he unlawfully retained.

In July 2014, Long was listed as the project leader on a lengthy research plan for CAS involving fourteen other individuals. The plan was replete with references to how the proposed research and development would benefit China. The plan stated: “The three major engine companies in the world, i.e. GE, Pratt & Whitney in the US and Rolls-Royce in the UK, are all using this technology. . . Our nation lacks the ability to process high performance components, such as airplane wings, tail hooks on carrier aircrafts, and blisks . . . Because of the technology embargo imposed by western developed countries, it is very difficult for us to obtain more advanced design and

manufacturing technology . . . This research project will increase our independent ability, efficient and quality in key component manufacturing."

On or about Aug. 12, 2014, the document on Distortion Modeling – the same document from which Long had sent the cover page to the SIA-CAS Director on Dec. 24, 2013 – was accessed on the external hard drive. Travel records and forensic analysis confirmed that both Long and the external hard drive were in China when this file was accessed.

On Aug. 19, 2014, Long returned to the U.S. from China through John F. Kennedy International Airport in New York. During a secondary inspection screening by U.S. Customs and Border Protection (CBP) officers, Long was found in the possession of a largely completed application for work with a state-controlled aviation and aerospace research center in China. The application highlighted certain parts of Long's work related to the F119 and F135 engines while at UTRC.

On or about Aug. 20, 2014, Long emailed an individual at a university in China, attaching an updated "achievement and future plan." In the plan, Long discussed his work related to the F119 and F135 U.S. military fighter jet engines and stated that he also had knowledge of unpublished UTRC projects in which the U.S. Air Force had shown interest.

On Nov. 5, 2014, Long boarded a flight from Ithaca, New York to Newark Liberty International Airport in Newark, New Jersey, with a final destination of China. During Long's layover in Newark, CBP officers inspected Long's checked baggage and discovered that it contained sensitive, proprietary and export controlled documents from another defense contractor, Rolls Royce.

Further investigation determined that the U.S. Air Force had convened a consortium of major defense contractors, including Pratt and Rolls Royce, to work together to see whether they could collectively lower the costs of certain metals used. As part of those efforts, members of the consortium shared technical data, subject to restrictions on further dissemination. Rolls Royce reviewed the documents found in Long's possession at Newark Liberty Airport and confirmed that it provided the documents to members of the consortium, which included Pratt. Rolls Royce further confirmed that Long was never an employee of Rolls Royce. A review of UTRC computer records indicated that Long had printed the documents while employed at UTRC.

Long was arrested on a federal criminal complaint on Nov. 7, 2014. A review of Long's digital media seized at the time of his arrest revealed voluminous files protected by the International Traffic in Arms Regulations and Export Administration Regulations, and voluminous files proprietary to various U.S. companies. In short, the investigation revealed that Long took his laptop and the UTRC external hard drive with him to China in 2014, at which time there was a substantial body of highly sensitive, proprietary and export controlled materials present on that digital media. UTRC has confirmed that the hard drive that Long unlawfully retained and accessed in China contained not only documents and data from projects on which Long worked while employed at the company but also from projects on which he did not work to which he would have had access.

A sentencing date has not been set. Long has been detained since his arrest.

This investigation is being led by the FBI in New Haven in coordination with Homeland Security Investigations in New Haven and Newark; the Defense Criminal Investigative Service in New Haven; the U.S. Air Force's Office of Special Investigations in Boston, Massachusetts; and, the Department of Commerce's Boston Office of Export Enforcement. U.S. Attorney Daly and Acting Assistant Attorney General McCord also thanked the FBI in Newark, Ithaca and Syracuse, New York, the U.S. Customs and Border Protection Service in New York and Newark, and the U.S. Attorney's Offices for the Northern District of New York and the District of New Jersey, for their efforts and assistance in this matter.

This case is being prosecuted by Assistant U.S. Attorneys Tracy Lee Dayton and Stephen B. Reynolds of the District of Connecticut, and Trial Attorneys Brian Fleming and Julie Edelstein of the National Security Division's

Counterintelligence and Export Control Section.

16-1506

Topic:

Counterintelligence and Export Control

National Security Division (NSD)

USAO - Connecticut

Updated December 19, 2016