Department of Justice

FOR IMMEDIATE RELEASE
WEDNESDAY, JUNE 18, 2008
WWW.USDOJ.GOV

NSD
(202) 514-2007
TDD (202) 514-1888

CHINESE NATIONAL SENTENCED FOR COMMITTING ECONOMIC ESPIONAGE WITH THE INTENT TO BENEFIT CHINA NAVY RESEARCH CENTER

First Sentencing under the Economic Espionage Act of 1996 and First Conviction Involving Military Source Code under the Arms Export Control Act

WASHINGTON -- Xiaodong Sheldon Meng, 44, a software engineer born in China and currently a resident of Cupertino, Calif., was sentenced today to a term of 24 months by the Honorable Jeremy Fogel, U.S. District Court Judge in San Jose and was also ordered to serve a three-year term of supervised release following his prison term; pay a fine of $10,000, and forfeit computer equipment seized in the case.

The sentence, the first handed down for a violation of the Economic Espionage Act of 1996 (18 USC Section 1831), was announced by Patrick Rowan, Acting Assistant Attorney General for National Security; Joseph P. Russoniello, U.S. Attorney for the Northern District of California; Arthur Cummings, Executive Assistant Director for the FBI's National Security Branch; and Julie L. Myers, Department of Homeland Security Assistant Secretary for U.S. Immigration and Customs Enforcement (ICE).

On August 1, 2007, Meng pleaded guilty to two national security violations: one count of violating the Economic Espionage Act and one count of violating the Arms Export Control Act and the International Traffic in Arms Regulations. Meng's conviction was the first involving military source code under the Arms Export Control Act and marked the second case in which there was a conviction under the Economic Espionage Act for misappropriating a trade secret with the intent to benefit a foreign government.

According to court records, Meng committed economic espionage by misappropriating a trade secret, known as "Mantis 1.5.5," from his former employer, Quantum3D Inc., with the intent to benefit a foreign government, specifically the People's Republic of China (PRC) Navy Research Center in Beijing. He did so by using the Mantis 1.5.5 trade secret as part of a demonstration project in attempting to sell products of his new employer, Orad, Hi-Tec Systems Ltd., which was a direct competitor of Quantum3D. The trade secret at issue, known as "Mantis," is a Quantum3D product used to simulate real world motion for military training and other purposes.

In addition, Meng violated the Arms Export Control Act by knowingly and willfully exporting to the PRC a defense article on the United States Munitions List (defense article viXsen) without authorization from the United States. The product viXsen is a Quantum3D visual simulation software program used for training military fighter pilots who use night visual sensor equipment, including thermal imaging.

According to court documents, the investigation established that Meng had, in fact, misappropriated two defense articles (specifically nVSensor, in addition to viXsen described above), at least six source code products which were also trade secrets, and more than one hundred materials and utilities belonging to his former employer, Quantum3D. Many of these misappropriated Quantum3D products were intended primarily for military purposes. For example, nVSensor is a Quantum3D product used to provide night vision simulation and is exclusively used in military applications for precision training and simulation applications.

The investigation also established that defendant Meng was assisting in developing two separate military proposals for two separate Air Forces in Southeast Asia involving visual simulation equipment and source code. Copies of two F-16 Full Mission Simulator proposals involving two different countries were found on Meng's laptop.

"Today's case demonstrates the importance of safeguarding sensitive U.S. military technology as well as trade secrets. It should also serve as a warning to others who would compromise our national security for profit," said Patrick Rowan, Acting Assistant Attorney General for National Security.

Mr. Rowan commended the teamwork of several agencies that worked on the case for nearly four years, including the U.S. Attorney's Office Computer Hacking and Intellectual Property (CHIP) Unit in the Northern District of California; the National Security Division and Criminal Division at the U.S. Department of Justice; the FBI, and ICE, as well Customs & Border Protection. The Department of State and the Department of Defense also provided assistance on the case. The U.S. Attorney's Offices in the Northern District of Alabama, District of Minnesota, and Middle District of Florida also joined the plea agreement as some conduct in the case occurred in those jurisdictions.

Joseph P. Russoniello, U.S. Attorney for the Northern District of California, stated, "In this case, a Silicon Valley trade secret was used in a demonstration project in Beijing with the intent to benefit the PRC Naval Research Center. Source code for military visual simulation programs to train military fighter pilots and restricted defense articles were also willfully exported outside the United States. We will continue to enforce the criminal laws against those who violate export restrictions and misappropriate our trade secrets. Many of the systems we protect are designed to safeguard our men and women in harm's way and compromising them significantly adds to the perils that they face in defending us. It is imperative that we vigilantly protect the intellectual property developed in the Silicon Valley and elsewhere in the country so as to maintain as our nation's military defense advantages, and to deter acts of aggression against vital American interests."

"ICE is committed to shutting down those who are willing to put America's national security on sale for a profit," said Julie L. Myers, Department of Homeland Security Assistant Secretary for ICE. "The export of U.S. military products and sensitive technology is controlled for good reason – in the wrong hands, these items could be used to harm America or its allies. Enforcing U.S. export laws is one of ICE's top priorities, and we will continue to work with our partners in law enforcement and industry to ensure that those who put our country at risk are brought to justice."

FBI Executive Assistant Director for the National Security Branch, Arthur Cummings stated, "Protecting our nation's most sensitive trade secrets and critical technology is at the core of the FBI mission. The FBI is committed to safeguard our country's economic well-being and national security."

Quantum3D, Inc., based in San Jose, California, has cooperated fully in the government's investigation. Quantum3D produces hardware and software components for simulation systems for commercial and military customers. Some of the products include high-end visual simulation systems, and interactive, open-architecture visual computing solutions, image generators, and embedded graphics subsystems.

Defendant Meng was ordered to surrender for this prison term on August 18, 2008. He has been out of custody after a $500,000 bond, secured by cash and real property, was posted at the beginning of the case.

The prosecution is being handled by Assistant U.S. Attorney Mark L. Krotoski, presently on assignment at the Computer Crime and Intellectual Property Section, with the assistance of Paralegal Lauri Gomez. Thomas P. Reilly, a Trial Attorney in the National Security Division's Counterespionage Section, also assisted on the case. The case was investigated by a team of agents from the FBI and ICE.

Prior Economic Espionage Prosecutions: The five cases charging violations of Section 1831 under the Economic Espionage Act (EEA) to date include:

- The first EEA Section 1831 indictment was returned on May 8, 2001, in the Northern District of Ohio in United States v. Okamoto and Serizawa. One defendant pleaded guilty to false statements and the other remains a fugitive. See: http://www.usdoj.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm.

- The second EEA Section 1831 indictment was filed on December 4, 2002, by the Northern District of California CHIP Unit in United States v. Fei Ye and Ming Zhong, CR 02-20145-JW. The first EEA convictions, involving defendants Ye and Zhong, were obtained on December 14, 2006. Sentencing in this case is pending. See: http://www.usdoj.gov/criminal/cybercrime/yeIndict.htm, and http://www.usdoj.gov/usao/can/press/2006/2006_12_14_ye.zhong.plea.press.html

- The Meng case was the third indictment under Section 1831 of the EEA, when charges were filed on December 13, 2006. It was also the first case to be

sentenced under the EEA and the second case resulting in an EEA conviction. See: http://www.usdoj.gov/criminal/cybercrime/mengCharge.htm ; and http://www.usdoj.gov/criminal/cybercrime/mengPlea.htm)

- The fourth indictment under Section 1831 of the EEA was filed on Sept. 26, 2007, by the Northern District of California CHIP Unit in United States v. Lan Lee and Yuefei Ge, CR 06-00424-JW. For more information, please view the following: http://www.usdoj.gov/criminal/cybercrime/liIndict.htm

- The fifth indictment under EEA Section 1831 was filed on February 6, 2008, by the Central District of California in United States v. Dongfan "Greg" Chung, No. SA CR 08-00024. For more information, please view the following: http://www.usdoj.gov/opa/pr/2008/February/08_nsd_106.html

###

08-545