COVINGTON

COVINGTON & BURLING LLP

E-ALERT | International Trade Controls

March 31, 2013

CHINESE NATIONAL SENTENCED TO NEARLY SIX YEARS IN PRISON FOR ILLEGALLY EXPORTING U.S. MILITARY TECHNOLOGY

On March 25, 2013, a federal district court in New Jersey sentenced Chinese national Sixing "Steve" Liu to 70 months in prison for export control and other violations. Liu was convicted in September 2012 of violating the Arms Export Control Act, the International Traffic in Arms Regulations, and the Economic Espionage Act, as well as transporting stolen property and lying to federal agents.

In a scheme to obtain employment in China, Liu stole thousands of electronic files detailing the performance and design of guidance systems for missiles, rockets, target locators, and unmanned aerial vehicles from his New Jersey-based employer, the Space and Navigation Division of L-3 Communications Holdings, Inc. ("L-3"). He then traveled to China with a computer containing the stolen files, and delivered presentations about the military technology detailed in the files at several Chinese universities.

Liu also was fined $15,000, and a hearing is scheduled for June at which he may be ordered to pay restitution.

BACKGROUND ON U.S. EXPORT CONTROL LAW

The Arms Export Control Act ("AECA") authorizes the President to control the export of U.S. military technologies, and the President has delegated this export authority to the U.S. State Department. Pursuant to the AECA, the State Department promulgated the International Traffic in Arms Regulations ("ITAR") to regulate the export of all articles and services designated by the State Department as having military significance, as well as software and technical data "directly related" to these articles and services. Articles designated as having military significance are listed on the United States Munitions List ("USML"), found at Part 121 of the ITAR.

The basic purpose of both the AECA and the ITAR is to safeguard U.S. national security and further U.S. foreign policy objectives by restricting exports of U.S. military technologies to non-U.S. persons, states, or other entities. Such exports are only permitted if they are specifically authorized by the State Department, or meet an exception found in the ITAR.

Willful violations of the AECA and ITAR may result in criminal fines for corporations or individuals of up to $1 million per violation, and individuals may be sentenced to up to twenty years in prison. In addition, civil penalties may be imposed of up to $500,000 per violation.

ALLEGED MISCONDUCT

L-3 is a global defense contractor with offices in the United States and abroad. L-3's Space and Navigation Division is based in New Jersey and researches, develops, and supplies the U.S. Department of Defense with precision pointing and land navigation systems, as well as integrated fire control systems.

According to the Second Superseding Indictment entered against Liu in the U.S. District Court of New Jersey, in March 2009 L-3 hired Liu as a senior staff engineer. In this position, Liu generated and handled ITAR-controlled technical data related to U.S. Department of Defense weapons programs.

The Second Superseding Indictment alleged that in November 2010, Liu copied to his personal laptop computer an electronic archive of his email correspondence from his work email account, as well as a shared electronic folder maintained on L-3's computer network containing approximately 36,000 files. Many of these emails and files contained ITAR-controlled technical data. Liu then traveled to China with his personal laptop but without a license from the Department of State to export the technical data that it contained. As a result, Liu was charged with and convicted of violating the AECA and ITAR by exporting to China ITAR-controlled technical data without proper authorization.

The Second Superseding Indictment also alleged that while in China, Liu gave presentations at several Chinese universities about the ITAR-controlled technology for which he exported technical data without State Department authorization. Liu allegedly gave these presentations in order to position himself for future employment in China. Liu was not, however, charged with crimes based on the presentations.

Notably, the Second Superseding Indictment emphasized that L-3 educated and trained Liu regarding the requirements of U.S. export control laws and the proper handling of export-controlled information. Liu also was required by L-3 policy to obtain approval from designated corporate officers before disseminating proprietary and export-controlled information outside of the company.

In addition to violating the AECA and ITAR, Liu was charged with and convicted of possessing stolen trade secrets in violation of the Economic Espionage Act ("EEA"), transporting stolen property, and lying to federal agents. The EEA make the theft of trade secrets a federal crime, and it imposes particularly severe penalties for "corporate espionage," which is the theft of trade secrets for the benefit of a foreign government.

IMPLICATIONS AND COMPLIANCE LESSONS

Liu's sentencing is the latest example that U.S. industry, and particularly the U.S. defense industry, appears to be increasingly targeted by individuals and corporations intent on stealing proprietary, classified, and export-controlled information. In the past four years, the Justice Department has charged nearly 100 individuals or corporations with unlawfully exporting to China ITAR-controlled technology or "dual use" technology controlled by the Export Administration Regulations administered by the U.S. Commerce Department, or stealing trade secrets or classified information for Chinese entities.

The case against Sixing Liu reinforces several export control compliance lessons:

- Even companies with robust policies and procedures to ensure export control compliance and prevent corporate espionage are vulnerable to employee theft of export-controlled, classified, and other proprietary information, and therefore must remain vigilant about continuing to strengthen and vigorously enforce these policies and procedures. Indeed, strong policies and procedures and effective training can help companies avoid liability even if they do not prevent the illegal conduct of a rogue employee,

- The importance of restricting employees' access to export-controlled, classified, and other proprietary information not necessary to carry out their job responsibilities. Much of the ITAR-controlled technical data Liu illegally exported to China was unrelated to Liu's job responsibilities for L-3.

- The importance of carefully screening new hires, and regularly re-screening existing employees, for warning signs that they will attempt to steal and potentially export such information. Liu allegedly stole proprietary and export-controlled information from previous employers in addition to L-3.

- Violations of U.S. export control laws are punished severely, and individuals who violate these laws can face lengthy prison terms.

* * *

If you have any questions concerning the material discussed in this client alert, please contact the following members of our international trade controls group:

Eric Carlson	86.10.5910.0503	ecarlson@cov.com
Peter Flanagan	202.662.5163	pflanagan@cov.com
Corinne Goldstein	202.662.5534	cgoldstein@cov.com
Peter Lichtenbaum	202.662.5557	plichtenbaum@cov.com
Kimberly Strosnider	202.662.5816	kstrosnder@cov.com
David Addis	202.662.5182	daddis@cov.com
Stephen Bartenstein	202.662.5471	sbartenstein@cov.com