from NSD Public Affairs

CHINA ILLEGAL EXPORT / ESPIONAGE TALKING POINTS
(April 3, 2008)

I: TALKING POINTS

A. Talking points from previous speeches / cleared statements on the China threat

- At recent press conference, Ken Wainstein, former Assistant Attorney General for National Security, stated: "While there are entities from over 100 different countries trying to get access to our secrets or our controlled technology, there are a number of countries that have proven themselves particularly determined and methodical in their espionage efforts. The Peoples Republic of China is one of those countries." (Ken Wainstein delivered remarks at Feb. 11, 2008 press conference on China espionage case).

- As the Director of National Intelligence testified last September, "China and Russia's foreign intelligence service are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities, and development projects, and their efforts are approaching Cold War levels." (September 18, 2007 Testimony before the House Judiciary Committee at page 8).

- The FBI has identified China as running an aggressive and wide-ranging effort aimed at acquiring advanced technologies from the United States. In July 26, 2007 testimony before the House Judiciary Committee, FBI Director Robert Mueller III, stated: "There is substantial concern. China is stealing our secrets in an effort to leap ahead in terms of its military technology, but also the economic capability of China. It is a substantial threat that we are addressing in the sense of building our program to address this threat."

- The Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE) reports that it has launched more than 540 investigations of illegal technology exports to China since 2000.

- The Defense Department this year in its "2008 Annual Report to Congress on the Military Power of the People's Republic of China" stated (pg 1) that China's army is pursuing a "comprehensive transformation from a mass army designed for protracted wars of attrition on its territory to one capable of fighting and winning short-term, high intensity conflicts along its periphery against high-tech adversaries."

- The DOD report adds (pg.1) that "China's near-term focus on preparing for contingencies in the Taiwan Strait, including the possibility of U.S. intervention, is an important driver of its modernization."

- Finally, the DOD report added (pg 1), "The pace and scope of China's military transformation have increased in recent years, fueled by the acquisition of foreign weapons, continued high rates of investment in its domestic defense and science and technology industries, and far reaching organizational and doctrinal reforms of the armed forces."

B. Talking points on DOJ prosecutions involving China

- We see these efforts in the prosecutions the Justice Department has been bringing into court lately. Since October 2006, we have filed charges in roughly dozens of cases involving illegal exports of sensitive technology to China, economic espionage involving trade secrets bound for China, or classic espionage involving China.

- The technology at issue in the export cases has ranged from battlefield night-vision equipment, to sensitive electronics with military communications applications, to accelerometers used in the development of smart bombs and missiles.

- In other cases, we have seen classic espionage networks in play, complete with traditional elements of spy tradecraft -- including foreign handlers, pay-offs, cut-out couriers and a compromised government employee – which have resulted in the penetration of our government's information security system and the passage of classified information.

- And finally we have seen economic espionage cases involving the theft of trade secrets from U.S. businesses that are routed to China. Sometimes these trade secrets, while not classified, contain data about our military systems that may be useful to China.

- These are all different approaches, but with the same objective in mind -- which is to get a hold of our sensitive technology, know-how, secrets or other data that may be useful.

C. Talking points on DOJ National Export Enforcement Initiative

- Given the severity of the threat posed by export control violators, we decided to institutionalize the steady expansion of our export control enforcement through a full-fledged national prosecution program.

- On October 11, 2007, the National Security Division joined his counterparts from ICE, the FBI, the Department of Commerce, the Department of Defense, and the Department of State to announce the advent of our nationwide Export Enforcement Initiative. This initiative has several different components, including:

- The creation of counter-proliferation task forces in districts across the country. We have roughly 15 task forces or working groups that are established and operating thus far.

- These task forces build on prior efforts in certain districts to bring together representatives from all the law enforcement agencies involved in export control. Under the leadership of U.S. Attorneys, these task forces foster multi-agency cooperation and provide a mechanism for member agencies to share investigative data, coordinate investigations, and follow up on leads from industry.

- We have also appointed a National Export Control Coordinator to oversee the development, implementation, and maintenance of the initiative.

- Another critical component of the initiative is expanded export control training for investigators and prosecutors around the country; as well as enhanced guidance on export control enforcement for federal prosecutors nationwide. The National Export Control Coordinator oversees training programs designed for those U.S. Attorneys' Offices that do not have extensive experience with such cases

- Furthermore, we are increasing coordination with the export licensing agencies to facilitate greater communication among the agencies. The NSD has initiated regular monthly meetings with the leadership of the enforcement elements of those offices

Ongoing

SELECT, PUBLIC DOJ CASES INVOLVING ILLEGAL EXPORTS, ECONOMIC ESPIONAGE, OR TRADITIONAL ESPIONAGE FOR CHINA

(October 2006 to April 3, 2008)

I. Espionage Cases

Defense Department Official Pleads Guilty to Espionage Charge Involving China – On March 31, 2008, Gregg William Bergersen, a former Weapons Systems Policy Analyst at the Defense Security Cooperation Agency, an agency within the Department of Defense, pleaded guilty in the Eastern District of Virginia to a one-count criminal information charging him with conspiracy to disclose national defense information to persons not entitled to receive it. Bergersen provided national defense information on numerous occasions to Tai Shen Kuo, a New Orleans businessman who is also charged with espionage in the case. Working under the direction of an official of the People's Republic of China (PRC), Kuo cultivated friendships with Bergersen and others within the U.S. government and obtained from them—for ultimate passage to the PRC—sensitive U.S. government information, including classified national defense information. Much of the information pertained to U.S. military sales to Taiwan and was classified at the Secret level. During the course of the conspiracy, Kuo bestowed on Bergersen gifts, cash payments, dinners, and money for gambling during trips to Las Vegas. Unbeknownst to Bergersen, Kuo passed along to the Chinese government official the information that Bergersen had provided him. In some meetings with Kuo, Bergersen cautioned that the information he was providing was classified. Bergersen faces up to ten years in prison when sentenced on June 20, 2008. Espionage charges are still pending against Kuo and an alleged conspirator, Yu Xin Kang, both of whom remain held without bond. Kang is a citizen of the PRC and a U.S. Lawful Permanent Resident, who allegedly served as a conduit of information between the Chinese official and Kuo. Press Releases:
http://www.usdoj.gov/opa/pr/2008/March/08_nsd_252.html
http://www.usdoj.gov/opa/pr/2008/February/08_nsd_105.html

II. Illegal Export & Economic Espionage Cases

Trade Secrets to China – On April 1, 2008, Hanjuan Jin, a naturalized U.S. citizen born in China, was indicted in the Northern District of Illinois for allegedly stealing business trade secrets from her employer, a telecommunications company in Chicago, and attempting to take these technical documents with her to

China for a new employer there. Jin allegedly possessed more than 1,000 electronic and paper proprietary documents when she attempted to travel one-way to China in Feb. 2007. The U.S. company had spent hundreds of millions of dollars on research and development for the proprietary data that Jin allegedly possessed without authorization. Jin was charged with three counts of theft of trade secrets. The investigation was conducted by the FBI, with assistance from U.S Customs and Border Protection.

U.S. Naval Warship Data to China – On March 24, 2008, Chi Mak, a former engineer with a U.S. Navy contractor, was sentenced in the Central District of California to 293 months (more than 24 years) in prison for orchestrating a conspiracy to obtain U.S. naval warship technology and to illegally export this material to China. Mak was found guilty at trial in May 2007 of conspiracy, two counts of attempting to violate export control laws, acting as an unregistered agent of the Chinese government, and making false statements. The investigation found that Mak had been given lists from co-conspirators in China that requested U.S. Naval research related to nuclear submarines and other information. Mak gathered technical data about the Navy's current and future warship technology and conspired to illegally export this data to China. Mak's four co-defendants (and family members) also pleaded guilty in connection with the case. The investigation was conducted by FBI, NCIS, and ICE.
Press releases: http://www.usdoj.gov/opa/pr/2008/March/08_nsd_229.html
http://losangeles.fbi.gov/dojpressrel/pressrel07/la060607usa.htm
http://www.usdoj.gov/usao/cac/pressroom/pr2006/146.html

Controlled Amplifiers to China – March 7, 2008: Wave Lab, Inc. of Reston, Virginia, pleaded guilty in the Eastern District of Virginia to illegally exporting of hundreds of controlled power amplifiers to China. The exported items, which have potential military applications, are controlled and listed on the Commerce Control List for national security reasons. Wave Lab purchased these items from a U.S. company and assured the company that the products would not be exported from the United States, but would be sold domestically. From February 2006 through October 2006, Wave Lab exported hundreds of the amplifiers without either a license or authorization from the Commerce Department.

Theft of Trade Secrets on U.S. Space Shuttle, Rocket Programs for China --February 11, 2008: Dongfan "Greg" Chung, a former Boeing engineer, is arrested in Southern California after being indicted on charges of economic espionage and acting as an unregistered foreign agent of the People's Republic of China (PRC), for whom he allegedly stole Boeing trade secrets related to several aerospace and military programs, including the Space Shuttle, the Delta IV rocket program, and the Air Force's C-17 aircraft. Chung, who was employed by Rockwell International from 1973 until its defense and space unit was acquired by Boeing in 1996, was named in an indictment in the Central District of California accusing him of eight counts of economic espionage, one count of conspiracy to commit economic espionage, one count of acting as an unregistered foreign agent without prior notification to the Attorney General, one count of obstruction of justice, and three counts of making false statements to the FBI. According to the indictment, individuals in the Chinese aviation industry began sending Chung "tasking" letters as early as 1979. Over the years, the letters directed Chung to collect specific technological information, including data related to the Space Shuttle. Chung responded in one letter indicating a desire to contribute to the "motherland." In various letters to his handlers in the PRC, Chung referenced engineering manuals he had collected and sent to the PRC, including 24 manuals relating to the B-1 Bomber that Rockwell had prohibited from disclosure outside of the company. Between 1985 and 2003, Chung made multiple trips to the PRC to deliver lectures on technology involving the Space Shuttle and other programs, and during those trips he met with agents of the PRC. The investigation was conducted by the FBI and the National Aeronautics and Space Administration. Press Release:
http://www.usdoj.gov/opa/pr/2008/February/08_nsd_106.html

4

Military Amplifiers to China -- January 25, 2008: Federal agents arrested Ding Zhengxing and Su Yang in Saipan pursuant to an indictment in the Western District of Texas that charges them with Arms Export Control Act violations. A third defendant, Peter Zhu, of Shanghai Meuro Electronics Company Ltd., in China, remains at large. The indictment alleges that the defendants attempted to purchase and illegally export to China amplifiers that are controlled for military purposes. The amplifiers are used in digital radios and wireless area networks. Zhengxing and Yang were arrested after they traveled to Saipan to take possession of the amplifiers. Press Release:
http://www.usdoj.gov/usao/txw/press_releases/2008/export_control_ind.pdf

Military Night Vision Technology to China -- December 2, 2007: Philip Cheng is sentenced in the Northern District of California to two years in prison and ordered to pay a $50,000 fine for his role in brokering the illegal export of a night vision camera and its accompanying technology to China in violation of federal laws and regulations. Mr. Cheng pled guilty on October 31, 2006, to brokering the illegal export of a Panther-series infrared camera, a device that makes use of "night vision" technology and is controlled for national security reasons. Mr. Cheng failed to obtain required government authorization prior to the export of the camera. Press Release:
http://www.usdoj.gov/usao/cau/press/2007/2007_12_03_cheng.sentenced.press.html

Military Night Vision Technology to China -- October 31, 2007: Bing Xu, of Nanjing, China, is charged by criminal complaint in the District of New Jersey with attempting to illegally export military-grade night vision technology from the U.S. to China. According to court documents, Xu arrived in New York from China to pick up the technology a day after his Chinese employer wired $14,080 to undercover federal agents as payment for the purchase of the restricted equipment. Press Release:
http://www.usdoj.gov/criminal/npftf/pr/press_releases/2007/oct/10-31-07bingxu-charge.pdf

U.S. Stealth Missile Data and Military Secrets to China -- October 26, 2007: Noshir Gowadia, an engineer who once worked on the B-1 bomber, is charged in a second superseding indictment in the District of Hawaii with an additional count of transmitting classified national defense information to China and two additional counts of filing false tax returns. Gowadia was charged in a superseding indictment in November 2006 with performing substantial defense related services for China by agreeing to design, and later designing, a cruise missile exhaust system nozzle that renders the missile less susceptible to detection and interception. Among other violations, Gowadia was charged in the first superseding indictment with willfully communicating classified national defense information to China with the intent that it be used to the advantage of China or to the injury of the United States, as well as unlawfully possessing classified information, and laundering funds paid to him by the Chinese government for his illegal defense work. Press Releases:
http://honolulu.fbi.gov/dojpressrel/pressrel06/defensesecrets110906.htm

Military Accelerometers with Missile Applications to China -- October 18, 2007: A federal grand jury in the Southern District of California returns an indictment charging Qing Li with conspiracy to procure the illegal export of military-grade accelerometers from the United States to the Republic of China. According to court papers, Li conspired with an individual in China to locate and procure Endevco 7270A-200K accelerometers for what her co-conspirator described as a "special" scientific agency in China. This accelerometer has military applications in "smart" bombs and missile development and in calibrating the force of nuclear and chemical explosions. Press Release:
http://www.usdoj.gov/opa/pr/2007/October/07_nsd_833.html

Economic Espionage and Theft of Trade Secrets – On Sept. 26, 2007, Lan Lee and Yuefei Ge were charged in a superseding indictment the Northern District of California on charges of economic espionage and theft of trade secrets. The indictment alleges that the pair conspired to steal trade secrets from two companies and created a new firm to create and sell products derived from the stolen trade secrets. The charges also allege that Lee and Ge attempted to obtain funds for their new company from the government of China, in particular China's General Armaments Division and China's 863 Program, otherwise known as the National High Technology Research and Development Program of China. Press Release: http://sanfrancisco.fbi.gov/dojpressrel/2007/sf092607a.htm

U.S. Military Source Code to China -- August 2, 2007: Xiaodong Sheldon Meng pleads guilty in the Northern District of California to violating the Economic Espionage Act to benefit China's Navy Research Center and violating the Arms Export Control Act for illegally exporting military source code. Meng is the first defendant in the country to be convicted of exporting military source code pursuant to the Arms Export Control Act. The code in question was designed for precision training of fighter pilots. Meng has not yet been sentenced. Press Release: http://www.usdoj.gov/usao/can/press/2007/2007_08_02_meng.guiltyplea.press.html

Restricted Technology to China -- August 1, 2007: Yang Fung, the president of Excellence Engineering Electronics, Inc., pleads guilty in the Northern District of California to a charge of illegally exporting controlled microwave integrated circuits to China without the required authorization from the Department of Commerce. Fung has not yet been sentenced.
Press Release:

Telecommunications Equipment from China to Iraq -- April 10, 2007: Andrew Huang, the owner of McAndrew's, Inc., an international export company, pleads guilty in the District of Connecticut to one count of making false statements to the FBI. Huang was charged in 2006 with operating as a representative for the Chinese Electronic System Engineering Corporation, the technology procurement arm of the government of China. According to court documents, Huang allegedly helped broker the illegal sale and transfer of millions of dollars worth of telecommunications equipment from China to Iraq between 1999 and 2001. On April 11, 2007, the Court sentenced Huang to two years of probation and imposed a $5,000 fine. Press Release:
http://newhaven.fbi.gov/dojpressrel/2006/nh050106.htm

$100 Million Penalty in Case Involving Illegal Exports of Military Night Vision Technology to China -- March 27, 2007: ITT Corporation, the leading manufacturer of military night vision equipment for the U.S. Armed Forces, agrees to pay a $100 million penalty and admits to illegally exporting restricted night vision data to China, Singapore, and the United Kingdom. The company also pleads guilty to charges that it omitted statements of material fact in required arms exports reports. The $100 million penalty is believed to be one the largest ever in a criminal export control case. As part of the plea agreement, ITT Corporation must invest $50 million of the penalty toward the development and deployment of the most advanced night vision systems in the world for the U.S. Armed Forces. Press Release: http://www.usdoj.gov/opa/pr/2007/March/07_nsd_192.html

Stolen Trade Secrets to Chinese Nationals -- December 14, 2006: Fei Ye and Ming Zhong plead guilty to charges of economic espionage for possessing trade secrets stolen from two Silicon Valley technology companies. The pair admitted that their company was to have provided a share of any profits made on

sales of the stolen chips to Chinese entities. The case marked the first convictions in the nation for economic espionage. The defendants have not yet been sentenced.
Press Release: http://www.usdoj.gov/criminal/cybercrime/yePlea.htm

Military Weapons Scopes to China – On Oct. 26, 2006, Wai Lim William Lam was charged in the District of Connecticut with attempting to smuggle weapons scopes, including submersible night-vision monocular devices, to Hong Kong. The investigation was conducted by DCIS, BIS, and ICE. Press Release: http://www.usdoj.gov/usao/ct/Press2006/20061211-3.html

Industrial Furnace to Missile Institute in China -- October 4, 2006: William Kovacs, the owner and president of Elatec Technology Corporation in Massachusetts, is sentenced to a year and a day in prison for illegally exporting a hot press industrial furnace to a research institute in China affiliated with that nation's aerospace and missile programs. Press Release:
http://www.usdoj.gov/usao/dc/Press_Releases/2006_Archives/Oct_2006/06369.html

7