U.S. Department of Justice

National Security Division

Washington, D.C. 20530

JUL 27 2009

Jenny Small
Judicial Watch
501 School Street, SW, Suite 725
Washington, DC 20024

Re: FOIA/PA # 09-037

Dear Ms. Small:

This is an interim response to your November 4, 2008, to the FOIA/PA Mail Referral Unit, Department of Justice, requesting access to "any and all records concerning assessments of illegally exported information and technology for military and space endeavors to China (reported by the Department of Justice)" from 2003 to the present. Your Freedom of Information Act request was forwarded to this office on December 11, 2008.

We have completed our search for responsive records within the Office of Intelligence (policy files), as well as relevant files within the Counterespionage Section. We have located nine documents that are responsive to your request. Six of these documents are being released in full and are attached for your convenience.

Two documents have been referred to other DOJ components for review and direct response to you. The remaining document is being release in part. The defendant's name and any other identifying information for sealed cases is exempt from disclosure pursuant to the District Courts' protective orders. These orders prohibit public release of this information. This exempt information is also properly withheld under Exemptions 5, 6 and 7(C) of the Freedom of Information Act, 5 U.S.C. §552 (b)(5), (b)(6), and (b)(7)(C). Exemption 5 pertains to certain inter- and intra-agency communications protected by the deliberative process privilege. Exemption 6 pertains to information the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties. Exemption 7(C) pertains to law enforcement information the disclosure of which could reasonably be expected to constitute an unwarranted invasion of personal privacy.

We note, we are still awaiting a response from the Counterterrorism Section and the Front Office. If you are not satisfied with this response, you may administratively appeal by

writing to the Director, Office of Information and Privacy, United States Department of Justice, 1425 New York Avenue, NW, Suite 11050, Washington, D.C. 20530-0001, within sixty days from the date of this letter. Both the letter and envelope should be clearly marked "Freedom of Information Act Appeal."

If you have any questions concerning your request, feel free to contact Theresa Crosland on 202-353-3092.

Sincerely,

Kevin Tiernan
Chief, Records and FOIA Unit

INTERIM RELEASE PACKAGE
FOIA # 09-037 SMALL

Re: Assessment of Illegally Exported Information to China

NSD FOIA 09-037-0001
thru
NSD FOIA 09-037-0009

FOIA Request #09-037 (Small)

RE: Assessment of Illegally Exported Information to China

NSD Doc #	Disposition
NSD FOIA REF 09-037-0001	DIRECT RESPONSE
NSD FOIA REF 09-037-0002	SEGREGATE - NSD, (b)(5), (b)(6) and (b)(7)(C)
NSD FOIA REF 09-037-0003	RELEASE
NSD FOIA REF 09-037-0004	RELEASE
NSD FOIA REF 09-037-0005	RELEASE
NSD FOIA REF 09-037-0006	DIRECT RESPONSE
NSD FOIA REF 09-037-0007	RELEASE
NSD FOIA REF 09-037-0008	RELEASE
NSD FOIA REF 09-037-0009	RELEASE

Pages 1 through 54 redacted for the following reasons:
- -
NSD FOIA 09-037-0001
DIRECT RESPONSE

COUNTERESPIONAGE SECTION (CES)
SIGNIFICANT EXPORT CONTROL CASES
SINCE SEPTEMBER 2001

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
09/29/01	U.S. v. Eugene Hsu, et al. District of Maryland Arms Export Control Act	Conspiracy and an attempt to export military encryption units to China through Singapore.	CUS	Eugene Hsu David T. Yang Wing Chang Ho a/k/a Charlson Ho	Guilty verdict 4/30/02 Guilty verdict 4/30/02 Sentencing 11/8/02 Fugitive
01/17/02	U.S. v. Klaus E. Buhler Middle District of Florida Arms Export Control Act	Conspiracy and attempt to export Chinook helicopter engines and parts and C-130 military aircraft engines to Libya.	CUS	K. Buhler	Pleaded guilty 4/17/03; sentenced to 30 months.
04/22/02	U.S. v. Joseph D'Allesio, et al. Eastern District of Texas Arms Export Control Act Theft of Government Property False statements - Conspiracy	Exportation of surplus military equipment from United States to Thailand. Scheme involved the theft of certain defense articles and false statements to further this scheme. Customs secured the return of the equipment to the United States.	CUS	Joseph D'Allesio Anthony Cordae	Pleaded guilty 3/17/03; sentenced to 2 years probation Charges dismissed 10/1/03.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
11/19/02	U.S. v. Stoelting Co. EAA	Exporting polygraph equipment to PRC without a license. 50 USC 1705	COM	LaVern Miller Stoelting Company	02/19/04 plea, 50 USC 1705; 03/03/05 sentenced to $18K fine, 12 months probation, & 500 hrs. community service. 02/19/04 plea, 50 USC 1705; 03/03/05 $20K fine & 2.5 years probation
12/10/02	U.S. v. Camnetics Manufacuring Corp. and William W. Manning, Jr. Et al Eastern District of Wisconsin Arms Export Control Act	Export of replacement parts for F-4 aircraft and Sikorsky helicopters to Vienna for transhipment to Iran.	CUS	Camnetics Manufacturing William W. Manning, Jr. Equipment and Supply International of North Carolina Andrew Adams Rick's Manufacturing and Supply of Oklahoma Jami S. Choudhury	Pleaded guilty to 18 U.S.C. 1001 and agreed to fine.
03/xx/03	U.S. v. Konstantine Katsaras (S.D. Florida) AECA	Conspiring to purchase/transport F-5 aircraft parts to Iran.	ICE	Konstantine Katsaras	Convicted of one count of conspiracy to violate AECA.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
03/06/03	U.S. v. David Hudak, Michael Payne, High Energy Access Tools, Inc., et al. District of New Mexico Arms Export Control Act; Possession of Unregistered Destructive Devices; Alien in Possession of Firearm; Use of Explosive Materials During a Felony; Conspiracy	Company and principals provided counter terrorism training to special forces of United Arab Emirates without State Department approval. Scheme involved the theft of classified training course from the Special Warfare Center at Ft. Bragg, NC. Provided classified training to foreign soldiers. Course was translated into Arabic and exported from the United States.	ICE ATF	David Hudak Michael Payne High Energy Access Tools, Inc. DLDT Corp.	Acquitted 11/19/03. Pleaded guilty 07/24/03 to one count 22 U.S.C. 2778. Dismissed Dismissed
03/20/03	U.S. v. Eric Chang, David Chu (D. Maryland) Conspiracy/AECA; money laundering	Conspired to acquire and export military radar detection electronics to Iran via Guam and Taiwan. "cavity-back spiral antennas"	ICE	En-Wei Eric Chang David Chu a/k/a Chu Loung Hsiang	Fugitive. NSD Arrested 2/22/03 in Guam. Pleaded guilty; sentenced to 24 months.
06/09/03	U.S. v. Mart Haller, Inc. and Allen Haller (D. Conn.) Conspiracy/AECA	Export of military components to Pakistan via U.A.E.	ICE	Mart Haller, Inc Allen Haller	Pleaded guilty.
06/12/03	U.S. v. Yasmin Ahmed and Tariq Ahmed (D. Conn.) AECA	Married couple purchased and attempted to export to Pakistan parts for Howitzer cannons, military radar, and armored personnel carriers	ICE	Yasmin Ahmed Tariq Ahmed	Pleaded guilty

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
07/10/03	U.S. v. Multicor I & II (multiple districts) AECA	Multi-district investigation of export of missile and fighter jet components to Multicor, Ltd. an Iranian front company in London, UK	ICE	numerous U.S. individual and corporate defendants	
08/21/03	U.S. v. Hazim Elashi 18 USC 371 18 USC 1001 50 USC 1701 18 USC 1957 see also US v. Ghassan Elashi	Re: family-run, Richardson, Texas, business, Infocom, conspiring to violate Export Administration Regulations and Libyan Sanctions Regulations.	COM	Hazim Elashi	7/7/04 trial Sentenced on 1/24/06 to 60 months imprisonment, 2 years probation, deportation upon release from custody.
09/23/03	U.S. v. Omega Engineering (D. Conn.) IEEPA/EAA	Company and its CFO willfully disregarded denial of export license and exported laboratory equipment with nuclear and non-nuclear applications to Pakistani Ministry of Defense	ICE	Omega Engineering	Sentenced to $313,000 criminal fine; $187,000 civil penalty. CFO sentenced to 5 years in prison and five years home confinement.
09/23/03	U.S. v. Suntek Microwave (N.D. California) EAR	EAR "deemed export" provision re: detector log video amplifiers (DLVA) shipments to PRC. 50 USC 1705	COM	Suntek Microwave Inc. Charles Kuan	04/26/04 pleaded guilty; $339,000 fine. 07/25/05 sentenced to 1 year in prison & $300 fine.
10/15/03	U.S. v. Sabri Yakou, Regard Yakou (D. D.C.) AECA	Brokering of sale of 6 armored patrol boats worth $11 million to Saddam Hussein regime in Iraq	ICE	Sabri Yakou Regard Yakou	Dismissed 7/24/06. Plea 7/20/06; 1 year probation.
11/12/03	U.S. v. Jami Siraj Choudhury (E.D. Wisconsin) AECA	Illegal export of military engine starters to Taiwan via California	ICE	Jami Siraj Choudhury	Sentenced to 37 months imprisonment, $2000 fine

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
11/13/03	U.S. v. Kovacs, Elatec Technology Corp. (D. Columbia) IEEPA/EAA Conspiracy	Exported sophisticated industrial furnace with potential missile applications to China after export license denied by Commerce	ICE	William Kovacs Stephen Midgley Elatec Tech. Corp.	05/28/04 plea agreement 18 USC 371; 10/04/06 sentenced to 12 months in prison, 3 years supervised release, 300 hours community service. 09/24/04 plea to 18 USC 1001; 01/10/05 $1500 fine & 12 months probation. Pending.
11/26/03	U.S. v. Zhan Gao (E.D. Va.) Export Administration Act (IEEPA) Tax Fraud	Exported Military Intel486 DX2 microprocessors to China without approval. Did not include proceeds from sale on income tax return.	CUS DCIS	Zhan Gao	Pleaded guilty to one count IEEPA and one count tax fraud; 15 months and $505,000 forfeiture. Husband, Donghua Hue, pleaded guilty to tax fraud.
12/xx/03	U.S. v. Avassapian (S.D. Fla.) Conspiracy/AECA brokering for Iran False Statement	Defendant was Tehran-based broker working for Iranian Ministry of Defense; met with UCA to solicit and inspect F-14 fighter components, military helicopters and C-130 aircraft which he intended to ship to Iran via Italy	ICE	Sherzhik Avassapian	Pleaded guilty 12/09/2004 to false statements charge

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
12/xx/03	U.S. v. Maine Biological Labs.	18 USC 2 & 3 18 USC 371, 1001, & 1341 21 USC 151 & 158 50 USC 2410	COM	Mark Dekich John Donahoe John Rosenberger Marjorie Evans Dennis Guerrette Thomas Swieczkowski Maine Biological Labs	11/09/04 plea to 18 USC 371; 9 months prison & $5000 fine. 06/28/05 plea to 18 USC 3 & 371; 1 year & $30,000 fine. 09/06/04 plea to 18 USC 2; probation & $10,000 fine. 04/01/04 plea; 1 year prison & $30,000 fine. 06/10/04 plea; 1 year prison & $10,000 fine. 06/10/04 plea; 1 year prison & $5,000 fine. 07/20/05 plea; $500,000 fine.
12/22/03	U.S. v. Hamad Lakhani (D.N.J.) Arms Export Control Act	Brokering shoulder-fired missiles for use by undercover agents posing as Al-Qaeda terrorists.	ICE/FBI	Hamad Lakhani	Guilty verdict 4/27/05
01/01/04	U.S. v. Asher Karni (D. D.C.) IEEPA/EAA	Export of triggered spark gaps (for nuclear weapons applications) to Pakistan via South Africa, U.A.E. Top Cape Technology	ICE DOC	Asher Karni (Israeli)	04/09/05 plea to 18 USC 371 & 50 USC 1701-1706. 08/04/05 sentenced to 3 years in prison.
01/09/04	U.S. v. Yaudat Mustafa Talyi (E.D. La.) IEEPA	Violation of temporary denial order filed by Department of Commerce. Transshipment of oilfield equipment through UAE to Libya.	ICE	Yaudat Mustafa Talyi	Pleaded guilty to two counts IEEPA. 10 months imprisonment. $25,000 fine. $75,000 civil fine.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
03/03/04	U.S. v. Drabos-Margaillon et al. (D. Arizona) Conspiracy –AECA	Conspiracy to export semi-automatic pistols and rifles to Mexico	ATF	Luis Hector Drabos-Margaillon Manuel Corella Luis Pericles Drabos Jorge Ortiz Luis Demetrio Drabos	Pleaded guilty; 36 months. Pleaded guilty; 37 months. Plea. Guilty verdict; 41 months.
03/18/04	U.S. v. Claudio Azocar and Thamara Ochsendorf (S.D. Fla.) Conspiracy Arms Export Control Act Possession of Unregistered Firearms	Conspiracy to export automatic weapons to Venezuela without license.	ATF	Claudio Azocar Thamara Ochsendorf	
04/15/04	U.S. v. Kohn and L&M Manufacturing Corp, Nesco NY, Inc. (D. Conn.) AECA	Purchased components for HAWK missiles, military radars, and F-4 Phantom fighter jets, and exported to Israeli company without a license	ICE	Leib Kohn L&M Manufacturing Nesco NY, Inc.	12/15/04 pleaded guilty (30 days imprisonment; 2 years probation; $25,000 fine) 12/15/04 pleaded guilty 12/15/04 pleaded guilty
05/05/04	U.S. v. Ali Khan 18 USC 371 50 USC 1705	Exporting aircraft parts to Iran without U.S.Gov't authorization.	COM	Ali Khan (CEO of Turboanalisis Inc. and Turbo Technologies LLC)	9/15/05 plea agreement.
05/10/04	U.S. v. Rotair Industries (D. Conn.) AECA	Military helicopter part manufacturer exported parts to Iran	ICE	Rotair Industries Wesley Harrington	Pleaded guilty 2 counts of illegal export to Iran $500,000 fine, export compliance program. Harrington pleaded guilty to obstruction

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
05/11/04	U.S. v. Kyriacou (E.D. Pa.) IEEPA/EAA IEEPA/OFAC Travel Act False Statement	Stolen Astroscope night vision lenses sold and shipped to undercover agents in Vienna, Austria for purported transshipment to Iran.	ICE	Erik Kyriacou	Pleaded guilty on 02/07/05 to 2 counts of violating IEEPA; sentenced 07/18/05 to 5 years' probation, 4 months home confinement and restitution.
05/18/04	U.S. v. Chu and Zhu (D. Massachusetts) Conspiracy AECA	Conspiring to purchase satellite and radar technology for export to China. Hong Kong New Crystal Int'l	ICE	John Chu Zhu Zhaoxin Sunny Bai	Chu acquitted 09/12/05. Zhu pleaded guilty 05/06/05 to 18 USC 371; sentenced 09/28/05 to 24 months. Bai is a fugitive.
06/xx/04	U.S. v. Davilyn Corp. (C.D. California) AECA	Exporting electron tube used in F-14 fighter.	ICE	Davilyn Corp.	05/10/05 pleaded guilty to one count of violating AECA. Agreed to $1,000,000 fine. Export Compliance Program.
06/03/04	U.S. v. Cheng and Shih (N.D. California) IEEPA/EAA money laundering	Brokering sale of military and commercial-grade night vision technology to China	ICE FBI COM IRS	Philip Cheng Martin Shih	Cheng trial ended with hung jury. Retrial expected. Shih died before trial.
06/29/04	U.S. v. David Tomkins (S.D. Fla) AECA	Attempted purchase of an A-37 fighter jet from UCA of ICE in 1991 to use in bombing of Columbian prison to assassinate Pablo Escobar (then chief of Medellin drug cartel) for Cali cartel; he became a fugitive, arrested on 8/31/03	ICE	David Tomkins	Pleaded guilty

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
07/06/04	U.S. v. Lara-Perez, et al. (D. Arizona) AECA	Conspired and attempted to export ammunition from the US to Mexico without license	ICE	Raul Lara-Perez Jesus Lara-Perez Ruben Naranjo-Gomez	
07/29/04	U.S. v. Universal Technologies, et al. (D. New Jersey) IEEPA/EAR	Export of items for defense weapons systems such as smart weapons, radar, electronic warfare, communications systems to China. Tengfang Terry Li, Zhonghe James Ji, Ronge Robin Tong, & Pearl Li (Nei-chien Chu) arrested in July 2004; charges pending.	ICE FBI COM	Universal Tech. Inc. Manten Electronics Inc Weibo Xu aka Kevin Xu Hao Li Chen aka Ali Chen Xiu Ling Chen aka Linda Chen Kwan Chun Chan aka Jenny Chan	5/01/06 prison sentences: 9/13/05 plea agreement; 5/1/06 sentenced to 44 months. 9/13/05 plea agreement; 5/1/06 sentenced to 30 months. 9/13/05 plea agreement; 5/1/06 sentenced to 18 months. 9/13/05 plea agreement; 5/1/06 sentenced to 2 years probation incl. 6 mo. home confinement
08/xx/04	U.S. v. Interaero, Inc. (District of Columbia) AECA	Components for HAWK missile, F-4 Phantom fighter jet, and F-5 Phantom/Tiger fighter jet exported to China between June 2000 and March 2001.	ICE	Interaero, Inc.	Sentenced on 11/18/04 to $500,000 fine and five years' corporate probation

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
08/03/04	U.S. v. Amanullah Khan, United Aircraft & Electronics (C.D. Ca.) AECA	Export of F-4 and F-5 fighter jets to China	ICE	Amanullah Khan United Aircraft & Electronics Ziad Jamil Gammoh Mexpar International Ahmad Nahardani Gabriela De Brea	Khan pleaded guilty 8/3/2004. UA&E pleaded guilty 8/3/2004. Gammoh pleaded guilty 6/24/2004. Mexpar sentenced to $75,000 fine and 3 years' probation 7/29/2004 Nahardani and De Brea pleaded guilty to AECA in September 2003 and sentenced to 21 months and 12 months in prison, respectively.
08/05/04	U.S. v. Ebara Int'l Corp. EAR/IEEPA	Export of cryogenic in-tank submersible pumps to Iran. 18 USC 371 18 USC 1956 50 USC 1701	COM	Ebara (Nevada) Everett Hylton	09/23/04 plea – 18 USC 2; 01/06/05 $6,300,000 fine. 09/23/04 plea to 18 USC 371; 12/07/04 $10,000 fine and 3 years probation.
08/10/04	U.S. v. Khalid Mahmood, Mohammed Sherbaf (N.D. Illinois) IEEPA/Iran	Attempted procurement of fork lift truck radiators for transhipment to Iran via Dubai	ICE	Khalid Mahmood Mohammed Sherbaf (?Sharbaf)	Mahmood pleaded guilty; 01/19/06 sentenced to 16 months. Sherbaf at large.
08/18/04	U.S. v. Mousavi-Khorasani, Mehrabian, et al. (E.D. Michigan) IEEPA/Iran Conspiracy Structuring	Conspiring to smuggle $44,000 in USD to Iran	ICE	Seyed Mousavi-Khorasani Zahra Mehrabian Najmeh Mousavi-Khorasani	

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
08/20/04	U.S. v. Tesmec	50 USC 1701, 1702, & 1705 15 CFR 764.2(a) & (c)	COM	Tesmec Inc.	12/03/04 plead agreement. $85,000 fine.
09/20/04	U.S. v. Victor Infante (E.D. N.Y.) AECA Drug offenses	Attempted export of assault weapons including the MAC-11 submachine gun, MP-5s, HK-94S, colt AR-15s and Uzi Model Bs to the Philippines importation of "meth" to NY, NJ	ICE	Victor Infante	Pleaded guilty to drug offenses
09/22/04	U.S. v. BEF Corp.	50 USC 1705 18 USC 1001	COM	BEF Corporation	11/12/04 plea agreement to 50 USC 1705(b) and 18 USC 1001. 04/01/05 $350,000 fine.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
09/30/04	U.S. v. Ning Wen,et al. (E.D.Wisconsin) Conspiracy IEEPA/EAA - 50 USC 1705, 2401 money laundering	Export of more than $500,000 of restricted electronic components (for military radar and communications applications) to China.	ICE FBI COM	Ning Wen Hailin Lin Jian Guo Qu Ruo Ling Wang	Wen convicted on 9/21/05; appeal denied 12/14/06. Sentenced on 1/18/06 to 60 months imprisonment, $50,000 fine and 2 years supervised probation. Plea agreement 6/29/05. Hailin Lin sentenced on 12/21/05 to 42 months in prison and $50,000 fine. Qu pleaded guilty to conspiracy on 5/5/05. Sentenced on 7/26/05 to 46 months, $2,000 fine and 2 years supervised release. Pleaded guilty to conspiracy on 5/5/05. Sentenced on 5/2/05 to six months in prison and a $1,500 fine.
10/06/04	U.S. v. Ting-Ih Hsu, et al. (M.D. FL) EAA conspiracy false statements	False statements in connection with export of low-noise amplifier chips to China (used in U.S. Hellfire missile). Azure Systems, Inc.	ICE	Ting-Ih Hsu Hai Lin Nee	10/06/04 plea to 18 USC 1001; both sentenced to three years' probation.
10/15/04	U.S. v. Hamid Butt (D. N.J.) AECA	Attempted to export F-14 electronic components to Germany w/o license, intended for Iran	ICE	Hamid Butt	

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
11/01/04	U.S. v. Nozzle Manufacturing, a.k.a. Monarch Nozzle (D. N.J.) IEEPA/Iran	Attempted to export oil burner nozzles to Germany, knowing they would be diverted to Iran	ICE COM	Nozzle Manufacturing Monarch Nozzle	1/20/05 plea agreement to 50 USC 1705 charge and $10,000 fine
11/10/04	U.S. v. Kwonhwan Park (D. Conn.) AECA	Exporting Black Hawk helicopter engines and other military items to China.	ICE	Kwonhwan Park	Pleaded guilty 11/19/04. Sentenced 08/30/05 to 32 months.
11/15/04	U.S. v. Erika Jardine (E.D. Pennsylvania) 22 USC 2778 - AECA 18 USC 641 selling U.S. property	Exporting controlled military equipment – Small Arms Protective Inserts (SAPIs)	ICE DCIS NCIS	Erika Jardine	11/09/05 pleaded guilty.
11/16/04	U.S. v. Carlos Melean Aviation Spares, Inc. (S.D. Fla.) AECA	Export of radar antennae control boxes for P-3 Orion surveillance aircraft to Spain	ICE	Carlos Melean Aviation Spares, Inc.	
12/09/04	U.S. v. Norsal Export	18 USC 1001	COM	Spector Int'l d/b/a Norsal Export	12/09/04 plea to 18 USC 1001; $57,000 fine.
12/17/04	U.S. v. Ghassan Elashi, et al. (N.D. Texas) 18 USC 371 50 USC 1705 - IEEPA 18 USC 1956 see also U.S. v. Hazim Elashi	Re: family-run, Richardson, Texas, business, Infocom, conspiring to violate Export Administration Regulations and Libyan Sanctions Regulations.	COM	Ghassan Elashi Bayan Elashi Basman Elashi	4/13/05 trial Sentenced on 10/12/06 to 80 months imprisonment 4/13/05 trial Sentenced on 10/12/06 to 84 months imprisonment 4/13/05 trial Sentenced on 10/12/06 to 80 months imprisonment

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
12/29/04	U.S. v. Valtex Int'l (D. Minn.)	Attempted export to PRC of thermal material to insulate satellites & missiles. 18 USC 1001 18 USC 1705	COM	Valtex Int'l Corp. Vladimir Alexanyan	02/02/05 plea to 18 USC 1705; 05/17/05 $250,000 fine & 5 years probation. 02/02/05 plea to 18 USC 1001; 05/17/05 $12,000 fine and 3 years probation.
01/13/05	U.S. v. Guillermo Cardoso-Arias (S.D. Fla.) AECA	Brokering and attempted export of 200 fully automatic AK-47 assault rifles for the AUC in Columbia (a designated FTO) to fight the FARC	ICE ATF DCIS	Guillermo Cardos-Arias	Pleaded guilty to illegal brokering and attempted export; awaiting sentencing
01/28/05	U.S. v. Sotoro Inami, Takashi Matsubara (E.D. Pa.) Conspiracy/AECA	Purchase and illegal export of military laser sights for M-16 and M-5 rifles	ICE	Sotoro Inami Takashi Matsubara	Arrested 2/17/04 in LA Fugitive.
02/02/05	U.S. v. Farahbakhsh, Fathololoomy, Diamond Technology and Akeed Trading Company (D. Connecticut) IEEPA/EAA Conspiracy	Exporting computer goods to Iran via the U.A.E. for entity affiliated with ballistic missile program in Iran. Also exported satellite communications system to Iran. 18 USC 371 18 USC 1705	ICE COM DCIS	Mohammed Farahbakhsh, Hamid Fathololoomy, Diamond Technology, Akeed Trading Co.	04/29/05 plea; 09/22/05 sentenced to 7 months prison.
02/11/05	U.S. v. Carlos Gammara-Murillo (M.D. Fla.) AECA material support to terrorists	Plotted to provide $4,000,000 of arms (grenades, assault rifles, grenade launchers, machine guns) to FARC in Columbia	ICE	Carlos Gammara-Murillo	Pleaded guilty

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
02/24/05	U.S. v. Ali Asghar Manzarpour (D. D.C.) IEEPA/Iran	Exported an experimental aircraft, the Berkut 360 single engine plane, from US to the UK, where it was re-booked for shipment to Iran, without OFAC license	ICE COM	Ali Asghar Manzarpour	Awaiting trial, pending extradition
03/01/05	U.S. v. Sevilla (N.D. Illinois) IEEPA/Iran	Attempted export of a universal testing machine to Iran without OFAC license	ICE	Juan Sevilla	09/14/05 pleaded guilty. Sentenced on 11/30/06 to a $10,000 fine, 5 years probation, six months home confinement and 100 hours community service
03/01/05	U.S. v. Matt Mihsen (E.D. Wisconsin) IEEPA/SALSRA Syria	Attempted export of munitions to Syria	ICE	Matt Mihsen	9/02/05 plea agreement to 18 USC 922 firearms offense Sentenced 10/21/05 to 7 months in prison and 1 year supervised release
03/01/05	U.S. v. Zhao Bing (Missouri)	Conspiracy to export restricted electronic components. 18 USC 371	FBI	Zhao Bing	06/30/06 sentence to 2 years probation & $200,000 fine
03/09/05	U.S. v. Metric Equip. Sales EAR/IEEPA	Exported oscilloscopes to Israel without a license.		Metric Equipment Sales	03/21/05 plea to 50 USC 1705 & 2410; 04/07/05 three years probation, $50,000 fine, 250 hours community service.
03/24/05	U.S. v. Vaezi, Tavakolian (D. Maryland) AECA attempt Conspiracy Money laundering	Attempted export of aircraft gunnery system components for F-4 and F-14 aircraft to Iran	ICE	Hossein Vaezi Abbas Tavakolian	Superseding indictment. Pleaded guilty and sentenced to 57 months' imprisonment

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
04/06/05	U.S. v. Gastech Engineering Corp. , Khosrowyar (N.D. Oklahoma) 18 USC 371 50 USC 1705 - IEEPA Iranian Trasactions Reg.	Gastech Engineering Corporation signed a $12 million contract with National Iranian Gas Company through a business it owned in Canada	ICE	Gastech Engineering Corporation Parviz Khosrowyar	1/11/06 Gastech pleaded guilty to 371 Conspiracy. Sentenced on 3/10/06 to 5 years probation, $5,000 fine, including forfeiture of $50,000 in proceeds and a $33,000 civil penalty to OFAC Khosrowyar failed to appear on previous indictment 03/28/05, superseding indictment filed 06/09/05 NSD
04/18/05	U.S. v. Correa-Arango, et al. (S.D. Florida) 22 USC 2778 - AECA 18 USC 371 - conspiracy	Conspiracy to purchase AK-47 assault rifles for shipment to Columbia terrorist group AUC	ICE	- Carlos Alberto Correa-Arango a/k/a Paco - Eduardo Marin-Mejias - Neuro Enrique Gonzalez - Angel Sisoy	06/08/05 Correa pleaded guilty. 08/08/05 Marin pleaded guilty to one count. 08/11/05 Gonzalez pleaded guilty to one count.
04/28/05	U.S. v. Quinn, et al. (D. District of Columbia) 50 USC 1705 - IEEPA 15 CFR 730-774 - EAR 31 CFR 560 - Iran transactions	Exported and attempted to export forklift components to Iran through UAE, without license from OFAC.	ICE COM	Robert E. Quinn Michael H. Holland Mohammed A. Sharbaf (see also Khalid Mahmood)	Quinn found guilty; 02/23/06 sentenced to 39 months, $6,000 fine Holland acquitted. Sharbaf at large.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
05/05/05	U.S. v. Wiseman, Woodson (D.District of Columbia) 22 USC 2778 - AECA	Sold militarized High-Mobility Multi-Wheeled Vehicles (HMMWVs) to foreign nationals in Middle Eastern countries	ICE	Ronald Wiseman Gayden Woodson	5/5/05 Wiseman pleaded guilty. Sentenced on October 24, 2006 to18 months imprisonment. 10/24/06 Woodson pleaded guilty. Scheduled to be sentenced on January 31, 2007
06/xx/05	U.S. v. George C. Budenz II (S.D. California) AECA – exporting defense articles w/o license	Exported to Malaysia amplifier used on GE J85 turbine jet engine (F-5 fighter) and nine nozzles for Honeywell T55 engine (Chinook helicopter); exported to Belgium afterburner actuator for J85 engine – at direction of Arif Ali Durrani.	ICE DCIS	George Charles Budenz II (see also Richard Tobey and Arif Durrani)	10/18/05 pleaded guilty to 3 counts of violating AECA. 07/17/06 sentenced to 1 year and $10,000 fine.
06/xx/05	U.S. v. Richard Tobey (S.D. California) AECA Conspiracy	Conspiring to export military aircraft components for F-5 and T-38 military fighter aircraft without a license from State for re-export to Iran	ICE	Richard Tobey (see also George C. Budenz II and Arif Durrani)	08/26/05 pleaded guilty to AECA conspiracy
06/28/05	U.S. v. PRA Worldwide, et al. (S.D. New York) 18 USC 1001 18 USC 371		COM	Igor Cherkassy	2/9/06 plea agreement 12/8/06 Sentenced 2 months imprisonment, three years supervised release, $5,000 fine
06/02/05	U.S. v. Univision Tech.	Exporting microwave equipment to PRC without a license.	COM	Zheng Zheng Univision Technology	06/28/08 plea to 18 USC 1001; $1,000 fine. 07/25/05 plea to 13 USC 305; $1,000 fine.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
06/05/05	U.S. v. Zhang, et al. (Conn. & New York)	Exporting restricted electronics components. 18 USC 371 conspiracy 18 USC 1343 wire fraud	FBI	Jason Zhen Zhang Jack Zhousen Tan Simon Shiyi Zhang	02/27/06 pleaded guilty to wire fraud. 06/05/06 sentenced to time served & returned to PRC. 07/18/06 convicted of conspiracy; sentenced to 18 months & $180K restitution
08/18/05	U.S. v. Wang and Chang (S.D. Florida) 18 USC 371 - conspiracy 50 USC 1702 - IEEPA	Conspired and exported radio communication encryption modules for use by Taiwan Coast Guard.	ICE COM	Chin Kan Wang Robin Chang	12/12/05 Wang pleaded guilty to conspiracy. Chang a fugitive NSD
09/xx/05	U.S. v. DiBattista (S.D. Florida) 22 USC 2778 - AECA 22 USC 401 - export of war materials 18 USC 371 - conspiracy	Brothers conspired to export AK-47's, AR-15/M-16's, and other guns to Venezuela.	ICE	Lucian DiBattista Romeo DiBattista	01/09/06 both pleaded guilty; sentenced to 46 months.
09/23/05	U.S. v. Arif Ali Durrani (S.D. California) 18 USC 371 - conspiracy 22 USC 2778 - AECA	Illegally exporting military aircraft components destined for Iran	ICE DCIS State	Arif Ali Durrani (see also George C. Budenz II and Richard Tobey)	06/05/06 sentenced to 150 months.
10/xx/05	U.S. v. Howard Hsy, et al. (Washington)	Export of night vision technology. 50 USC 2410 Conspiracy to violate EAA and AECA.	FBI	Howard Hsy Donald Shull	12/06/05 plea; 03/23/06 sentenced to 2 yrs probation, comm. service & $15K fine. 10/11/05 plea; 02/17/06 sentenced to 2 yrs probation & $5K fine.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
10/21/05	U.S. v. M.R. Faria (E.D. Pennsylvania) IEEPA	Shipping agricultural commodities to Iran via Dubai, UAE.	ICE	M.R. Faria	10/21/05 plea agreement.
10/26/05	U.S. v. Koh (S.D. New York) 18 USC 371 50 USC 1705 18 USC 1956	Diverting U.S. aircraft parts for transshipment to Iran. Aviation Tec	COM	Ernest Koh Marcus Chua	5/18/06 trial; 10/13/06 sentenced to 52 months imprisonment. 04/29/05 plea to 18 USC 371; sentenced to 16 months in prison & deported to Singapore.
11/xx/05	U.S. v. Kal Nelson Aviation (C.D. California) AECA	Dealing with aircraft components used in military systems, including F-14 Tomcat.	ICE	Kal Nelson Aviation, Inc.	01/12/06 pleaded guilty to one corporate count of violating AECA. Agreed to $1,000,000 fine.
12/08/05	U.S. v. David and Ali Talebi (S.D. California) 22 USC 2778 - AECA 22 CFR 127.1 conspiracy 28 USC 2461 forfeiture	Attempted to ship ITAR controlled aircraft parts (utilized on F-14, F-4, and F-5)	ICE DCIS	David Talebi Ali Talebi	02/14/06 pleaded guilty to AECA and forfeited $69,800. Sentencing scheduled for 05/08/06.
02/xx/06	U.S. v. Reza Tabib (C.D. California) IEEPA	Attempted to ship F-14 components to Germany, destined for Iran.	ICE	Reza Tabib Teri Repic-Tabib	06/05/06 pleaded guilty to violating IEEPA. 12/04/2006 pleaded guilty to making false statement.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
02/09/06	U.S. v. Moo, Voros et al. (S.D. Florida) 18 USC 201 - bribery 18 USC 371 - conspiracy 18 USC 951 - foreign agent 22 USC 2778 - AECA	Attempted export of defense articles (F-16 engine, Blackhawk helicopter engines, cruise missiles, air-to-air missiles) and brokering the sale and transfer of the same to the PRC	ICE DCIS	- Ko-Suen Moo a/k/a Bill Moo - Maurice Serge Voros	07/24/06 Moo sentenced to 78 months, $1,000,000 fine, forfeit his interest in $350,000 seized. Voros at large.
03/16/06	U.S. v. Mohammad Fazeli (C.D. California) 50 USC 1705 - IEEPA 18 USC 371 18 USC 1001	Attempting to export pressure sensors used in aircraft black box data recording devices to Iran	ICE	Mohammed Fazeli	Pleaded guilty 05/08/06 to IEEPA. Sentenced on 08/07/06 to one year and one day imprisonment and a $3000 fine
04/11/06	U.S. v. Chia Kia Cheng (S.D. California) 18 U.S.C. § 2778 18 U.S.C. § 1956	Attempted export of M4 Carbine fully-automatic rifles and M4 Commando fully-automatic rifles to Indonesia with laundering money as part of the illegal export.	ICE	Chia Kia Cheng, aka Ronald "KC" Chia	Pleaded guilty to one count of money laundering in violation of 18 U.S.C. § 1956 on June 19, 2006.
04/18/06	U.S. v. Browne, Nouri (E.D. Pennsylvania) 18 USC 371 - conspiracy to violate 50 USC 1705(b) 18 USC 1956	Conspiracy to export goods to Iran in violation of IEEPA and the Iranian Sanctions Regulations and money laundering (Nouri)	ICE	Amy Browne Akbar Nouri	Attempting to obtain jurisdiction over Nouri, a citizen of Iran

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
04/20/06	U.S. v. Hadianto Djoko, et al. (E.D. Michigan) 18 USC 371 - conspiracy Money laundering 22 USC 2778 - AECA	Conspiracy to export munition list items (radar parts; Sidewinder missiles; Heckler & Koch handguns, submachine guns, & sniper rifles) to Indonesia without a license.	ICE DCIS	Hadianto Djoko Djuliarso Ibrahim Bin Amran Ignatius Ferdinandus Soeharli David Beecroft	01/18/07 pleaded guilty to two counts: (1) conspiracy to violate the AECA and (2) conspiracy to launder money. Pleaded guilty on 12/20/06 to two counts: (1) conspiracy to violate the AECA and (2) conspiracy to launder money. Sentencing is pending. 01/xx/07 pleaded guilty to one count of conspiracy to violate the Arms Export Control Act. Pleaded guilty on 11/15/06 to conspiring to violate the AECA, was sentenced to 8.5 months incarceration to be followed by 2 years of supervised release with a special condition that prohibits him from reentering the United States after his deportation.
04/05/06	U.S. v. Med Tek, et al 50 USC 1705 - IEEPA		COM	Dr. Joseph Thomas	11/14/06 plea agreement. Sentencing pending
04/26/06	U.S. v. Huang 18 USC 371 18 USC 1001 50 USC 1705 - IEEPA	Export of telecommunications equipment.	COM FBI	Andrew Huang NSD	12/11/06 plea agreement. Sentencing pending

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
09/05/06	U.S. v. Mendoza, et al. (S.D. Florida) 18 USC 371	Attempting to export 4 riflescopes without license to Columbia.	ICE	Mendoza, Marta Becerra, ? Riccardi, Pascual	09/05/06 arrested. 09/05/06 arrested. 11/21/06 warrant issued.

NSD

09/26/06	U.S. v. Yssouf Diabate, (S.D. California) 22 U.S.C. 2778(b)(2), (c); 22 CFR 121.1, 123.1, 127.1(a)(1) , and **18 U.S.C. 554** [new].	Attempted export of small arms and magazines to Côte d'Ivoire in violation of the Arms Export Control Act	ICE	Yssouf Diabate	02/09/07 convicted.
09/28/06	U.S. v. Haji Subandi, et al. (D. Maryland) 18 USC 371 22 USC 2778 - AECA 18 USC 2339(B) 18 USC 1956	Conspiracy to export USML items to Iran, Vietnam, Laos, Indonesia and Sri Lanka in violation of AECA, and on behalf of Liberation Tigers of Tamil Eelam, a FTO designated by DOS	ICE FBI DCIS NCIS	Haji Subandi Reinhard Rusli Helmi Soedirdja Erick Wotulo	03/08/07 pleaded guilty. Pleaded guilty. Pleased guilty. 02/23/07 pleaded guilty. Additional suspects arrested in Guam.
09/29/06	U.S. v. Lincoln & Stephenson (N.D. Illinois) IEEPA 1001	Export of metal cutting machinery to Iran.	ICE	Stephen Lincoln David Stephenson	Court refused to accept guilty plea to 1001; deferred prosecution for three years.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
10/17/06	U.S. v. Ghassemi, et al. (S.D. California) 18 U.S.C. § 371 18 U.S.C. § 1956 22 U.S.C. § 2778 18 U.S.C. § 554.	Conspiracy to export munition list items - including accelerometers and gyroscopes for missiles and spacecraft - to Iran without a license.	ICE	Jamshid Ghassemi (Iranian national) Aurel Fratila	Jamshid Ghassemi: Detained in Bangkok, Thailand and resisting deportation to the U.S. Aurel Fratila: Under supervised release in Bucharest, Romania. DOJ is seeking his arrest and deportation to U.S.
10/25/06	U.S. v. Chi Mak, et al., (C.D. California) 18 U.S.C. § 2778 18 U.S.C. § 957 18 U.S.C. § 951 18 U.S.C. § 1001	Acting as agents of China without notifying the Attorney General; conspiring to export controlled technical data relating to Navy ships and submarines to China without obtaining a license from the State Department; possession of a laptop computer and encryption software in aid of China; and making false statements to investigators.	FBI, NCIS ICE	Chi Mak Rebecca Laiwah Liu Tai Wang Mak Fuk "Lilly" Li Yui "Billy" Mak	Guilty verdict at trial. Others defendants pleaded guilty.
10/25/06	U.S. v. William Wai Lin Lam (D. Connecticut) 18 USC 554 Smuggling goods from US	Sale of stolen USML items (military combat optics) to UCA and attempted export of night vision equipment w/o license	ICE DCIS	William Wai Lin Lam	12/11/06 plea agreement. 3/9/07 sentenced to 14 months.
11/08/06	U.S. v. Menchaca (W.D. Texas) AECA 554	Export of semi-automatic handguns and assault rifles to Mexico.	ICE	Victor Menchaca	Plea negotiations ongoing.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
12/02/06	U.S. v. Andrew Freyer, et al., (C.D. California) 18 U.S.C. § 371 50 U.S.C. §§ 1701-1706, 31 C.F.R. §§ 560.204, 560.701, 31 C.F.R. §§ 575.411, 575.701, 18 U.S.C. § 2(a),(b)	Conspiring to export Crane Pacific valves to Iran and Iraq through intermediary countries; Australia and England	COM	Andrew Ward Freyer Sharon Kay Doe	Trial Pending
12/13/06	U.S. v. Xiaodong Meng (N.D. California) 22 USC 2778 - AECA 18 USC 1831 - Econ. Espionage 18 USC 1832 theft of trade secrets 18 USC 2314 ITSP 18 USC 371 18 USC 1001	Theft of proprietary software concerning night vision and thermal imaging (some of which is USML controlled for export by ITAR) and attempted sale of same to the PRC	ICE CBP	Xiaodong Meng aka Sheldon Meng	
01/10/07	U.S. v. Mustafa & Sehweil (E.D. Louisiana) 371 IEEPA 1001	Export of oil production machinery to Lybia.	ICE	Jamie Radi Mustafa, Nureddin Shariff Sehweil	
01/22/07	U.S. v. Tabbaa 22 USC 2151	Attempting to export Mercedes Benz automobiles to Syria without DOC license.	COM ICE	Tabbaa, Ghassan Joseph	01/22/07 sealed warrant for arrest.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
02/07/07	U.S. v. Tappin et al. (W.D. Texas) AECA	Re: sale of Hawk missile batteries.	ICE USAO	Tappin, Chris Gibson, Robert Caldwell, Robert	Caldwell convicted; Gibson pleaded guilty; Tappin being extradited.
03/28/07	U.S. v. Latifi (N.D. Alabama) 22 USC 2778 - AECA	Indicted for illegally exporting sensitive military technology (Blackhawk helicopter drawings), fraud involving aircraft parts, and submitting false docs to Govt.	NASA DCIS ICE FBI IRS	Latifi, Alexander Nooredin Axion Corporation	03/28/07 indicted.
09/18/07	U.S. v. Schenk (N.D. Florida) AECA	Selling stolen military equipment (night vision ANVIS-9) overseas.	USAF ICE	Schenk, Leonard	09/18/07 pleaded guilty; sentenced to 234 months.
10/14/07	U.S. v. Li (S.D. California) 18 USC 371 - AECA	Attempting to procure military grade accelerometers for China.	ICE	Li, Qing	Sentenced to 12 months.
11/08/07	U.S. v. Roach et al. (S.D. Florida) 18 USC 554	Conspiracy to smuggle weapons into Canada in exchange for money and narcotics.	ATF ICE	Roach, Gary Frazier, Laron	01/07/08 both found guilty.
11/20/07	U.S. v. Boushvash (S.D. New York) 22 USC 2778 18 USC 1956	Re: military aircraft components for Iran.	ICE	Boushvash, Yousef	Fugitive.
12/19/07	U.S. v. Gholikhan (S.D. Florida) 18 USC 371 22 USC 2278	Re: illegal export of night-vision goggles to Iran.	ICE	Gholikhan, Shahrazad	04/25/08 pleaded guilty to 18 USC 371.

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
01/18/08	U.S. v. Mejia (S.D. Florida) 22 USC 2278	Attempting illegal export of USML items; handguns for Guatemala.	ICE ATF	Mejia, Osmar Needleman, Victor	Mejia pleaded guilty. Needleman pleaded guilty.
03/20/08	U.S. v. Yahya et al. (S.D. Florida) 18 USC 371 50 USC 1702 & 1705	Re: Mayrow General Trading in Dubai; electronic components for IEDs in Iraq/Afghanistan.	DOC ICE	Yahya, Ali Akbar Yaghmaei, F.N.	Fugitives.
03/27/08	U.S. v. Xu (D. New Jersey) 18 USC 554	Re: night vision and radar technology for China.	ICE	Xu, Bing	
04/08/08	U.S. v. Spitz (S.D. Florida) 22 USC 2778 - AECA/ITAR	Brokering arms deals re: munitions & Russian MI-24 & MI-8T helicopters to embargoed nations.	ICE	Spitz, Peter	Trial scheduled for Sept.
04/15/08	U.S. v. Peng et al. (S.D. New York) 22 USC 2778 - AECA 18 USC 554 - smuggling	Re: international sale of stolen military commodities, e.g. infrared laser aiming devices.	ICE	Peng, Yen-Po Liu, Peter	Liu pleaded guilty.
05/16/08	U.S. v. Orellana (S.D. Florida) 22 USC 2778 18 USC 554	Re: rifles and ammunition destined for Guatemala.	ATF ICE	Orellana, Juan Luis	Trial scheduled for Sept.

NSD

Date Indicted	Cases	Charges	Investi-gative Agency	Defendants	Disposition
		NSD			

JULY 2008

China export

RELEASE

Competing with Intelligence: New Directions in China's Quest for Intangible Property and Implications for Homeland Security†

Robert Slate

INTRODUCTION

Some enterprises do not hesitate to use illegal means to collect intelligence from their competitors, making trade secret protection increasingly challenging and urgent.

—China Business Training Course on Competitive Intelligence Practices
Shanghai, Oct. 17-18, 2008[1]

Chinese executives' intense desire to succeed globally, combined with the Chinese government's encouragement and support,[2] has driven some companies to develop corporate competitive intelligence (CI) programs that increasingly rely on illegal human and technical intelligence collection methods[3,4] to acquire intangible property from U.S. companies and government agencies. The plethora of industrial espionage cases involving Chinese companies in recent years reveals extensive Chinese government involvement in such activity[5] and the role of CI in facilitating the transfer of U.S. proprietary technology from civilian to military uses.[6] Against this backdrop, the United States faces a rising national security threat from Chinese corporations that employ robust CI programs to enhance illegal company- or government-directed espionage and intellectual property (IP) theft and infringement. The complicated and global character of this phenomenon[7] requires that the U.S. government rethink the traditional intelligence community (IC) approach to collection and analysis of intelligence on China and the implications for homeland security.

This article draws upon a body of Chinese literature on CI to explore the role of CI in helping China to conduct industrial espionage and acquire U.S. IP and illustrate how the study of Chinese CI can help the U.S. government and business make sense of future trends in Chinese industrial espionage. Chinese CI theory and practice is pushing Chinese intelligence in new directions;[8] however, this trend has gone relatively unnoticed in the U.S. intelligence and academic communities, probably because CI is largely viewed as the domain of private sector and professional organizations in the United States.[9] Despite Chinese corporations' growing reliance on CI, and the significant role it has played in corporate successes, many U.S. companies remain relatively unfamiliar with the state of Chinese corporate intelligence and the evolving risks for U.S. corporations.

INTANGIBLE THREAT

The 17th Century French missionary Louis Le Comte wrote in his memoirs that trade and commerce "is the soul of the (Chinese) people" and "the *primum mobile* of all their actions."[10] China's trade and commercial genius has certainly played a major role in the

spectacular rise of China's economy and its integration with the U.S. economy over the last several decades. Some observers view China's growing stake in America's economic system as an extremely positive development for the United States, while others see Beijing as a military, economic, and technological threat. Most would probably agree, however, that China's growing economic power[11] and massive annual trade surplus with the United States – $250 billion and growing – puts China in a position to affect the United States economy in ways considered improbable in the past.[12]

Chinese firms' increasing involvement in corporate spying and IP theft in America raises the stakes of the trade deficit problem with China and is the source of a great deal of concern for U.S. homeland security. Chinese corporations that use IP theft and infringement as components of their overall business model, and effectively employ corporate intelligence programs to that end, are damaging the foundations of the American corporate world: intangible property.

Most of the value in corporations, particularly in America, remains in intangible property. The term "intangible property" is generally used to refer to the following non-physical assets, such as intellectual property (e.g., patents, copyrights, trademarks, and trade secrets), legal rights (e.g., leases, contracts, and licenses), relationships (e.g., supply and custom distribution chains) and brands. According to a 2006 Brand Finance report in 2006, 62 percent of the value of corporations around the globe is based on intangibles ($19.5 trillion of global market value).[13] U.S. corporations have 75 percent of their value tied up in intangibles.[14] Not surprisingly, intangible property accounts for 98 percent of the U.S. technology sector.[15]

Intellectual property receives a lot of attention because its misappropriation can devastate companies, especially those in IP industries, and can have a disproportionate impact on countries like the United States, where IP factors so prominently in the overall economy. U.S. IP industries, for example, have been responsible for approximately 40 percent of the total growth of the U.S. economy.[16] The International Intellectual Property Alliance (IIPA) released an economic study in 2007 that assessed U.S. copyright industries (e.g., entertainment software, motion picture, business software, and recording) as contributing more job growth, gross domestic product (GDP), and foreign exports and sales to the U.S. economy than any other industry; they contributed about $1.38 trillion to U.S. GDP, employed 11.3 million workers, and accounted for approximately $110.8 billion in foreign sales and exports in 2005.[17]

OVER 300 HUNDRED YEARS OF COUNTERFEITING EXCELLENCE

Le Comte extolled Chinese merchants for their commercial genius, but suggested they focus much of their "labor and natural industry" on dishonest business practices and counterfeit "almost everything they vend."[18] He writes: "(Chinese merchants) counterfeit Gammons of Bacon so artificially, that many times a Man is mistaken in them; ... It is certain a Stranger will be always cheated, if he buy alone, let him take what care he will."[19]

Remarkably, Le Comte's observations from over 300 years ago remain valid today, and manifest themselves in the intractable problem U.S. companies encounter doing business with China: how to take advantage of China's vast trade and commercial

potential without losing much of the intangible value of their corporations to counterfeiting and other forms of infringement.

Chinese counterfeiting and piracy levels are extremely high. According to the IIPA's 2008 Special 301 Report, Chinese copyright piracy cost U.S. copyright industries almost $3 billion in 2007; piracy levels reached 90 percent of published records and music, 80 percent of business software and 95 percent of entertainment software. According to the U.S. trade representative's report to Congress on China's World Trade Organization compliance in 2004, the value of Chinese counterfeit products brought into the U.S. market reached $134 million. Chinese counterfeiting also limits demand for legitimate U.S. IP products globally, which damages company revenues and, by extension, the U.S. economy. The U.S. Department of Commerce, for example, reported that Chinese counterfeiting cost the U.S. economy about $20-24 billion in 2004.

Counterfeiting is not limited to Chinese street merchants. Chinese multinational corporations (MNC) are significant contributors to the overall counterfeiting of high-tech products. Cisco Systems filed an IP infringement claim in 2003 against Huawei Technologies (a powerful Chinese MNC that produces telecommunications and networking equipment) for copying patented Cisco technologies, user manuals, and the source code used for Huawei's counterfeit routers. In a 2005 interview with PriceWaterhouseCoopers, Warren Heit, a partner at White & Case, states that display cases at some of Huawei's offices contained 'perfect' knock-offs of Cisco telecom and Polycom equipment.[20]

Some Chinese MNCs view both legal IP development and illegal IP theft and infringement as extremely important components of their business models and key to their long-term profitability and survival. Huawei's business model, for example, is partly based on selling counterfeit products in developing countries with poor IP protection. As Heit suggests: "Huawei is saying to itself... 'I am going to knock (Cisco) products off and to the extent the IP law allows me to practice in these areas, I'm going to go there...Cisco, maybe you can have the U.S., but I'll take you everywhere you haven't gone.'"[21]

Chinese corporations' counterfeiting of high-tech equipment and IP theft raises concerns beyond economic loss. Counterfeit computer components from China, for example, could be used to compromise U.S. corporate and government computer networks and cause military systems to fail.[22] The U.S. government in early 2008 seized $76 million worth of counterfeit Cisco routers, switches, WAN interface cards, and gigabit interface converters, which were purchased by the U.S. Naval Academy, U.S. Naval Air Warfare Center, General Services Administration, U.S. Naval Undersea Warfare Center, and defense contractor Raytheon, among others.[23] Melissa Hathaway, director of the Director of National Intelligence's (DNI) cyber security office, commented on the government's seizure of over 400 counterfeit routers: "Counterfeit products have been linked to the crash of mission-critical networks, and may also contain hidden 'back doors' enabling network security to [be] bypassed and sensitive data accessed [by hackers, thieves, and spies]."[24]

COUNTERFEITER, HACKER, SOLDIER, SPY

Chinese espionage directed against U.S. government and corporate targets is well-documented in the recent literature. U.S. Immigration and Customs Enforcement officials have investigated over 540 instances of illegal technology exports to China, which often involve Chinese corporations. The *Washington Post* published an article in April 2008 describing twelve cases of Chinese espionage that have occurred since March 2007. The charges range from illegal export of warship technology and source codes for simulation software for the precision training of fighter pilots, to theft of trade secrets from two companies on behalf of a Chinese military program. Joel Brenner, the head of the counterintelligence office of the DNI, states: "Espionage used to be a problem for the FBI, CIA and military, but now it's a problem for corporations...It's no longer a cloak-and-dagger thing. It's about computer architecture and the soundness of electronic systems."[25]

The U.S. Defense Department and IC claim that China is America's most serious cyber security threat.[26] The Office of the DNI, in response to a *Business Week* inquiry, stated that computer intrusions have been successful against a wide range of government and corporate networks across the critical infrastructure and defense industrial base.[27] A recent *Business Week* special report revealed Chinese hackers may have recently sent an e-mail attachment containing the malicious computer code to an executive at Booz Allen Hamilton, a $4 billion U.S. corporation, in an attempt to infect the company's computer network and acquire sensitive information. According to the report, hackers have launched numerous similar attacks on U.S. companies and government agencies for the last several years; the Departments of Defense, State, Energy, Commerce, Health and Human Services and Treasury, and corporations Boeing, Lockheed Martin, General Electric, Raytheon and General Dynamics, are some of the known victims. The U.S. government reported the occurrence of 12,986 cyber intrusions and other cyber security events on government and defense contractor networks; U.S. military networks experienced a 55 percent increase in attacks.[28] O. Sami Saydjari, a former National Security Agency (NSA) official, suggests the scale of organized Chinese hacking activities – much of which involves the Chinese military[29]– is having a devastating impact on U.S. government and corporate computer networks.[30]

A number of Chinese companies aggressively employ intelligence collection methods that cross the line of propriety and legality, and some of them are also IP infringers. According to the U.S. Department of Justice, U.S. auto-parts manufacturer Metaldyne, one of only two corporations in the world capable of transforming powdered metal into high-performance engine components, was seriously damaged when one of its former engineers gave proprietary information to potential Chinese competitors. A Huawei employee illegally took photos of Fujitsu circuit boards at Supercomm in 2003; *Business Week* speculated that the employee may have also collected proprietary information from AT&T, Cisco, Lucent, Nortel, and Tellabs.[31] The U.S. software maker 3DGeo Development Inc. caught several trainees of the Chinese state-owned oil company Petro China Co. trying to access 3DGeo's secure computer systems; one was sentenced to two years in prison in 2004.[32] As a result of the increased incidents, the FBI decided in 2007 to identify the ten highest-value U.S. corporations (including General Electric,

DuPont and Corning) in the respective areas of the FBI's fifty-six field offices throughout America and brief those corporations on the threat.[33]

Chinese government research institutes are also actively involved in trade secret theft. The FBI and other U.S. government agencies recently identified about 150 individuals and businesses involved in illegally transferring aerospace and weapons technology to China and Iran; the espionage may have benefited Chinese government's space program.[34] Most notably, the FBI arrested physicist Shu Quan-sheng, the president of a National Air and Space Agency (NASA) subcontractor, for allegedly exporting restricted U.S. technology to China to assist the development of China's Long March V heavy booster. According to the federal claim, Shu allegedly transferred sensitive data on the components of a specialized cryogenic hydrogen tank to the People's Liberation Army's General Armaments Department and its 101st Research Institute. In a separate case, the U.S. Department of Justice (DOJ) reported in June 2008 that China's Naval Research Center acquired Quantum3D Inc.'s Mantis 1.5.5 and viXsen trade secrets – software programs used to simulate real world motion and train military fighter pilots – from Xiaodeng Sheldon Meng, a Chinese software engineer and former employee of Quantum3D Inc.[35]

STRATEGIC ROAD AHEAD: CHINESE CORPORATIONS MUST LEAD THE WAY

The late Professor Zheng Chengsi, father of IP in China and former director of the Intellectual Property Office of the Chinese Academy of Sciences (CAS), declared China's economic growth in the 21st Century will largely depend on its ability to manage intangible property and produce enterprises capable of successfully engaging in global IP competition.[36] Zheng's work at CAS persuaded the State Council to develop China's first *National Intellectual Property Strategy* – promulgated in June 2008 – and his intellectual imprint is reflected in the *Strategy's* emphasis on transforming the way companies create and acquire IP overseas.[37] Section 2 (12) of the *Strategy* emphasizes the importance of making the corporation "the principal entity in the creation and utilization of intellectual property." The *Strategy* also bears the mark of China's national security experts in that it calls upon government agencies and enterprises to make more effective use of IP for national defense and encourages the development and use of civilian IP for military purposes.[38]

The *Strategy* highlights the importance of improving China's capacity to create IP and Chinese-developed standards,[39] in which increased research and development (R&D) plays an integral role.[40] On this front, Beijing has been very successful in inducing most large U.S. high technology firms to invest heavily in R&D in China – largely in the form of high-technology R&D programs and centers in exchange for market access and financial incentives – which is gradually helping China close the gap between basic research and bringing inventions to market. In addition, U.S. R&D activities in China not only help Chinese subsidiaries improve their own R&D programs,[41] but could also indirectly help China's defense-modernization efforts.[42]

> [L]ocal Chinese employees working at foreign R&D centers may gain an in-depth understanding of how foreign technologies are developed and function. In some instances, R&D activity has included integrating foreign technology with local

> systems or making foreign technology compatible with Chinese technical standards. This latter form of knowledge transfer (systems and standards integration capabilities), in particular, could be of potential use to China's defense modernization goals, especially in developing asymmetric capabilities. For this and other reasons...extensive knowledge transfers through R&D in China could pose risks for long-term US security as well as economic interests. [43]

China spends heavily on R&D to improve China's capacity to rapidly absorb and adopt foreign technologies that can advance civilian and defense technology and IP development. According to the 2007 OECD report, China has become one of the most R&D intensive countries in the world, second only to the United States; China's R&D spending in 2007 surpassed Japan's for the first time. China's R&D spending could increase 24 percent in 2008 to $216.8 billion, which is roughly 18 percent of R&D spending worldwide.[44] China's total R&D spending in 2007 reached approximately $175 billion (an increase of nearly $155 billion in R&D spending since 2003). U.S. and Japanese spending during that same period totaled about $353 billion and $143.5 billion, respectively.[45] The European Commission recently assessed that, if China continues to increase its R&D spending at the current pace, China could match the EU in R&D expenditure as a percentage of GDP by 2009.[46] It is important to note, however, that government-sponsored R&D focuses primarily on applied research and technology development (the government used less than 6 percent of total R&D funding for basic research in 2002 and 2003).[47]

Chinese corporations are becoming the most important contributors to the R&D spending in China. According to the Research Institute of Industrial Economics and Orebro University in Sweden, Chinese companies conducted about 68 percent of China's total R&D in terms of spending in 2005, which highlights the dramatic shift from a government-centered to a corporate-dominated innovation system.[48]

Comparisons of China's R&D expenditures with developed countries do not account for the large disparities between China and the West in the quality and cost of research staff. As Dr. Xu Zhijun, chief marketing officer of the Chinese multinational telecommunications giant Huawei argues, because of China's low labor costs and access to high-quality researchers, Huawei may have spent only $1.1 billion in R&D last fiscal year, but that is equivalent to about $4 to $5 billion spent by western rivals such as Cisco.[49]

As suggested later in this article, the global economic downturn has important implications for Chinese corporate R&D programs. Chinese companies will have to make hard choices about R&D funding, and many of them will probably choose to focus exclusively on combining in-house R&D with imported technology to avoid the high costs and risks associated with basic and more innovative research. (This R&D strategy has been heavily used by legitimate companies and counterfeiters in the past for reverse engineering purposes).[50]

THE STRATEGIC VALUE OF COMPETITIVE INTELLIGENCE

Beijing's push to make IP the strategic imperative of government agencies and corporations, as manifested in the *Strategy*,[51] has had a significant impact on Chinese companies. Many Chinese executives, seeking to fulfill the government's desire that

their enterprises become the driving force behind China's technological innovation and IP creation, have established new competitive intelligence (CI) units or expanded their existing programs.[52] Chinese companies have reportedly intensified efforts to hire qualified Chinese CI personnel to fill a growing number of CI collection and analysis positions.[53]

Zhong Tianwei, the Guangzhou branch manager of Beijing TRS Information Technology Company,[54] notes that many domestic enterprises can attribute their successes to CI.[55] Competitive intelligence can help companies determine competitors' R&D capabilities, keep informed of competitors' product developments, assess competitors' product performance, design new technologies and products, assess a competitor's management strategies and decision-making capabilities, plan and manage R&D activities, create advanced S&T-based strategies, identify competitors interested in strategic alliances, and improve a company's capability to protect its intellectual property from illegal human and technical collection.[56]

The Mandarins' Perspective on Competitive Intelligence

Chinese government officials, scholars, and business strategists have written extensively about CI and recognize how it can help China (as it did Japan) achieve its IP goals and eventually become an economic superpower.[57] China's vigorous promotion of CI, and its subset competitive technical intelligence (CTI), have helped make these important topics of concern in China.[58] The Chinese Ministry of Ordnance Industry's Intelligence Research Institute, National Defense Science and Industry Scientific and Technical Intelligence Bureau, and the State Science and Technology Commission initiated a study comparing domestic and foreign intelligence research and held a series of seminars on strategic intelligence research and development from 1991 to 1994, resulting in a change in the direction of Chinese intelligence research work: competitive intelligence became its new focal point.[59]

Since the mid-1990s, a growing number of Chinese PhD dissertations have focused on CI and the use of intelligence to advance China's national interests.[60] Many of these students have gone on to become influential in business, government, and academia, and have helped push the theoretical development of corporate intelligence in China. Dr. Chen Feng, for example, who received his PhD from Beijing University and wrote his dissertation on CI in China with the assistance of his advisor Liang Zhanping, director of China's Institute of Information Science and Technology, is now a CAS associate researcher and senior consultant to Ding Lu Management Consultants, Ltd. and has advised Chinese high-technology firms how to set up CI programs.[61]

U.S. and Chinese scholars have provided a myriad of definitions of CI and CTI. Corporate CI can generally be defined as activity related to the collection, processing, exploitation, analysis, and dissemination of information and finished intelligence on corporate competitors and pertinent industries that could impact a firm's competitive situation. How narrowly or broadly a corporation defines the term depends on the company's mission and the goals of its intelligence programs; generally, more resources and funding are required to meet intelligence goals that are broader in scope. W. Bradford Ashton of Pacific Northwest National Laboratory and Richard Klavans of the Center for Research Planning define CTI as "business sensitive information on external

scientific or technological threats, opportunities, or developments that have the potential to affect a company's competitive situation."[62]

Chinese scholars have generally accepted the above definitions, but have added caveats of their own. Chinese and U.S. scholars also agree that corporate intelligence does not and should not include unethical or illegal forms of intelligence collection, such as unauthorized monitoring of phone and internet communications, trade secret theft, etc. However, some Chinese scholars concede that a gray area exists in CI, where reverse engineering and IP transfer may take place without necessarily breaking the law and the benefit to public interest may override the ethical considerations.[63]

Chinese academics point out that company intelligence efforts are necessarily proprietary and need to be protected. The company's sources and methods of collecting, processing, and analyzing information, and the intelligence derived from such activities, is confidential and usually well-guarded because unauthorized disclosure could negatively impact the company's competitive position. This is primarily why Chinese companies are so interested in "anti-competitive intelligence" (also referred to as counterintelligence) programs: to help protect against IP loss in the "gray area." This is discussed with some frequency in the Chinese literature.[64] (As will be suggested later in this article, U.S. companies could also benefit from increased emphasis on counterintelligence programs.)

Chinese Competitive Intelligence in Practice

Chinese corporate intelligence in practice can differ substantially from how it is described in scholarly works. Although Chinese scholars stress that corporate intelligence programs must employ ethical and legal intelligence techniques and methods to produce intelligence, mounting evidence suggests Chinese firms are increasingly using their intelligence units to enhance the effectiveness of their illegal activities. Chinese espionage cases involving IP theft from U.S. companies since 2007 indicate the emphasis China places on illegal corporate intelligence, the great risks China is willing to take to acquire U.S. IP, and the disregard it has for the global IP system (note that the Chinese government denies any illegal conduct).

As discussed, Chinese executives and managers hope to transform their companies into global competitors (86 percent of Chinese executives interviewed for a McKinsey survey in 2008 indicated they had global ambitions). They view the development of corporate intelligence programs as a means to improve strategic management and help identify struggling U.S. firms to purchase. This ambition can drive them to turn otherwise ethical CI programs into illegal collection platforms. 'The Chinese are out to develop a modern economy and society in one generation,' notes Joel Brenner. 'There is much about their determination that is admirable. But they're also willing to steal a lot of proprietary information to do it, and that's not admirable.[65]

The most robust Chinese corporate intelligence units are likely located in R&D centers overseas (often called "listening posts"), where the company can most effectively collect intelligence from its competitors and leverage the deep expertise of its many high-quality and relatively low-cost scientists and engineers to analyze and evaluate the technology and IP the company purchases or steals.[66] The Chinese literature suggests the intelligence units' internal processes are generally similar to those described in some of the most prominent works on corporate intelligence in the west.[67] The organization of

some of the units may differ somewhat from those in the West, but they likely combine personnel with formal intelligence training and those who are experts in their given technical or scientific fields to conduct intelligence collection, processing and exploitation, analysis, production, and dissemination.[68] Personnel assigned to listening posts can use their legal collection and analysis of patents, standards, business and market data, and information to inform illegal collection activities and vice-versa. They can also rely on scientific and technical assistance from their company headquarters, some of which are located in high-technology science parks in China and so have direct access to world-class government research institutes and universities (many of which employ scientists, engineers and academicians who have undoubtedly developed a corpus of useful knowledge and techniques related to obtaining proprietary and classified information from U.S. corporate and government laboratories).[69, 70]

These listening posts – some of which may receive Chinese government intelligence and military financial support and collection guidance[71] – may also employ illegal technical collection techniques (such as hacking) in the United States to obtain proprietary information from key U.S. competitors. Brenner claims Chinese hackers, on behalf of a Chinese corporation, hacked into "a large American company" to obtain sensitive company information prior to an impending business negotiation between the U.S. and Chinese companies. In a *National Journal* article, Brenner recounted the following incident: "The [U.S. business] delegation gets to China and realizes, 'These guys on the other side of the table know every bottom line on every significant negotiating point.' They had to have got this by hacking into [the company's] systems."[72]

Chinese illegal technical collection threatens U.S. corporate facilities worldwide and puts U.S. R&D centers operating in China at risk. In late 2007, Jonathan Evans, the director general of Britain's domestic intelligence agency MI5, warned 300 firms operating in the UK of growing evidence that state-sponsored Chinese hackers were attacking corporate networks and stealing proprietary information.[73] Although U.S. technology firms likely have physical and operational security procedures in place in their facilities inside China, they are probably no match for China's corporate and government intelligence services – among the most effective in human and technical intelligence collection in the world.[74] Microsoft Corporation, which intends to invest one billion dollars in China R&D over the next three years, will undoubtedly be a target for domestic Chinese competitors.

RETHINKING THE INTELLIGENCE PARADIGM

Roger George, senior analyst at the CIA's Global Futures Partnership, argues the traditional intelligence paradigm, which was relatively successful in dealing with state-centric problems, is less effective at collecting and analyzing global and transnational phenomena. These emerging challenges are 'blind spots' that are difficult for analysts operating under traditional organizational and functional constraints to identify and understand.[75] The global character of Chinese corporate espionage challenges the effectiveness of traditional U.S. intelligence and law enforcement efforts.[76] An analysis of recent studies and press reports also suggests the U.S. IC and law enforcement communities still lack sufficient resources and expertise to effectively collect and

analyze data and information on Chinese espionage activities directed against U.S. companies worldwide.

Although the *Cox Report* was written a decade ago, many of its findings are relevant today. The report acknowledges the U.S. government cannot "completely monitor PRC activities in the United States" because of the scope of China's "decentralized collection efforts."[77] According to the report, the CIA, Department of Commerce, FBI, and DoD never considered Chinese technology acquisition an intelligence priority. They failed to establish collection requirements to obtain information on Chinese government or commercial efforts to acquire U.S. technology companies, identify and obtain advances in U.S. technology, or establish business relationships with U.S. high-technology companies. Nor did U.S. agencies establish requirements to examine commercial affiliations between Chinese foreign nationals and U.S. companies.[78] The Select Committee of the U.S. House of Representatives determined U.S. government agencies only conducted "narrow" or "reactive" monitoring of Chinese business activities rather than taking more proactive measures.[79] "[T]here is little or no coordination," states the report, "within the U.S. Government of counterintelligence that is conducted against the PRC-directed efforts to acquire sensitive U.S. technology."[80]

The IC's scientific and technical (S&T) intelligence framework – an outgrowth of the Cold War which largely collects and analyzes key S&T data and information within a classified system[81] to understand foreign weapons platforms and identify emerging S&T threats,[82] remains ill-suited to adequately handle evolving Chinese corporate espionage focused on IP theft and infringement. Under this S&T paradigm, Chinese CI would not likely be considered relevant for S&T collection and analysis (the IC would probably view it as a business or management issue) and IP would be treated primarily as an economic, legal, and trade-related matter. Chinese academics, government, and industry, however, encourage greater collaboration between government and industry intelligence programs[83] and largely view S&T and IP as inseparable, whether from an intelligence or economic perspective.

Dr. Rob Johnston, in his 2005 study on analytic culture in the IC, suggests there is a separation of the domains of S&T and economic intelligence and expertise within the analytic community.[84] To the extent that situation now exists and is not mitigated through collaboration, some S&T and economic analysts, who are looking at data and information from the perspective of their areas of focus and expertise, may overlook critical IP and R&D data and information that directly impacts analytic judgments on S&T developments in China.[85] An economic analyst who has spent a career learning the tenets of economic analysis may not understand how unique IP and R&D data and information could inform S&T intelligence analysis,[86] or consider how Chinese corporate intelligence impacts trade and innovation. If such issues are not overlooked, they would probably fall under the purview of analysts working on transnational matters; those analysts may or may not have extensive scientific, technical, or economic expertise, or even speak Chinese (RAND suggests the IC's expertise and focus on S&T analysis and the assessment of foreign R&D programs has decreased).[87] [88]

The lines between Chinese intelligence, military, and commercial activities are not truly 'blurred.' The blurring of the lines cited in the *Cox Report*[89] demonstrates how the IC has tried to apply a Western construct to understanding Chinese business and intelligence practices. As suggested from the evidence in previous sections of this article,

there are no strict legal lines separating Chinese intelligence activities from the corporate world as exist in the United States. Chinese corporations are always subject to extensive government influence and control, and many companies prefer having close links to the government for protection and access to resources and information that can give them a competitive advantage.

The barrier the IC has created between S&T and IP could create an imbalance in the allocation of resources and funding for collection and analysis of the issues. This could influence which U.S. agencies handle certain requirements and how IC offices are organized and staffed to deal with particular analytic problem sets; it could hinder collaboration and increase analytic error.[90]

The IC lists its intelligence collection priorities in the National Intelligence Priorities Requirements Framework (NIPF), which emphasizes about twelve priority intelligence targets; countries, or issues out of 150, according to a 2008 study by the RAND Corporation.[91] The NIPF ranking of the relative importance of these priorities affects government resource allocations and those of the most critical importance to the country receive more funding for collection and analysis. [92] The RAND study characterizes priorities such as terrorism, WMD proliferation (an S&T intelligence issue) and China as NIPF "crosscutting problems or theme-areas."[93] The study points out the "NIPF has great value for many uses, but it also provides an incentive to reduce spending resources on all but the hottest current priorities, often at the expense of deeper assessments of longer-term challenges."[94]

Many U.S. policymakers tend to look to organizations such as the Department of State, DOJ, and the U.S. Patent and Trademark office for expertise on IP and other IP-related issues. Trade secret theft – one area of IP most often discussed in the intelligence context – is largely seen as the purview of agencies dealing with domestic counterintelligence matters, such as the FBI.[95] Because of this, some other IC agencies, which are in the position to assist the FBI, might not be doing so because of cultural or institutional barriers.

It is also difficult for the U.S. government to impress upon companies the seriousness of the threat and persuade them to respond appropriately. Some U.S. corporations might be unwilling to assist the FBI or Department of Homeland Security (DHS) – for example, by revealing the fact a Chinese corporation has stolen proprietary information through human or technical intelligence collection methods – to avoid potentially negative repercussions for their business interests in China or damage to shareholder confidence.[96]

There are also indications that U.S. companies are still not taking the Chinese seriously. A recent McKinsey survey suggests that while U.S. executives view Chinese corporations as a significant threat, few (28% of respondents) have taken sufficient steps to counter the threat because of a perception that Chinese firms are relatively weak in product quality, marketing, and brand development. The report observes: "This lackluster reaction to the global ambitions of Chinese companies raises the question of whether business executives elsewhere are setting themselves up for some unhappy competitive surprises."[97]

THE COMING STORM

Chinese leaders have made it clear that they want to reinvent China's role in the world economy and move from dependence on foreign technology and direct investment to a country that rivals the United States in terms of industrial and technological power. They recognize that this requires promoting and rewarding scientific discovery and true innovation, increasing IP ownership, developing new technology standards, and making it possible for Chinese corporations to play an even greater role in foreign technology acquisition and IP transfer. China has made considerable advances in developing favorable national and local S&T, IP, and business policies, and has increased its emphasis on education and R&D.

Chinese companies have shown they can effectively absorb and adopt U.S. technology and IP to push innovation. According to Curtis Carlson and William Wilmot of SRI International, the company that pioneered innovations such as the computer mouse and robotic surgery, China is working with preeminent partners around the globe to create the future technologies, attaining parity with the United States in some areas such as nanotechnology.[98] Along these lines, Frans van Houten, CEO of the European semiconductor company NXP, states China is now home to about 400 semiconductor firms that design chips and some of these companies will rapidly become top-notch innovators.[99] Motorcycle suppliers, designers, and manufacturers, in Chongqing, China, have collaborated to develop a unique entrepreneurial network and business model called 'localized modularization', which allows manufacturers to request parts from suppliers without specifying details; i.e., makers note the size and weight of the parts in their orders and suppliers decide what parts to provide. This push to innovate is contributing to the rapid expansion of China's patent system: Chinese domestic patent applications grew from 165,773 in 2001 to 470,342 in 2006.[100]

Some observers are very optimistic about China's largely untapped capacity to innovate. The National Science Foundation estimates China could graduate about four-times more engineering PhDs than America in the next several years. Based on their observations of the work of Chinese scientists, engineers, and researchers, Carlson and Wilmot believe the Chinese are just as creative as their Western counterparts; there is ample evidence of creativity and entrepreneurial ambition in Chinese firms.[101] Many Chinese engineers and scientists who received their PhDs in the United States, some of whom played important roles in successful innovations in U.S. high-tech firms, are now returning to China.[102]

At the same time, Chinese industrial espionage and IP misappropriation, often done with the support or knowledge of the government, shows China is also willing to disregard the traditional rules of the game when convenient and take great risks to acquire U.S. government secrets and corporate proprietary information to the detriment of U.S. national security. As demonstrated earlier, a number of the most well-known and powerful Chinese corporations actively engage in IP misappropriation, theft, and reverse engineering and solicit IP transfer from their foreign competitors' former employees. To date, intense U.S. corporate and government pressure on the Chinese government to improve the enforcement of IP rights has had limited results. Clearly, the blowback for Chinese espionage has not been severe enough for some Chinese companies to stop their illegal activities.

Against this backdrop, one wonders how long U.S. technology firms – despite their current comparative advantage in S&T and IP – will be able to withstand Chinese competition. Many U.S. scholars and business leaders might argue that most U.S. firms will not succumb to Chinese competitive pressure until China improves its capability to innovate and strengthen its IP base vis-à-vis the United States. This could take several decades at a minimum. However, some of these same U.S. observers (perhaps due to bias, mirror imaging, apathy or hubris) fail to take seriously a question that weighs heavily on the minds of many Chinese executives with global aspirations and government leaders who want to turn China into a superpower: "How can we further improve the effectiveness of our CI programs, whether it be through legal or illegal means, to continue to close the IP gap with U.S. companies?"

ECONOMIC DOWNTURN CREATES OPPORTUNITIES

The global economic crisis is having a major impact on Chinese companies and trade. Chinese President Hu Jintao recently told members of the Communist Party that the global economic downturn is hurting China's competitive advantage in trade and threatens Party legitimacy and ability to rule.[103] Chinese leaders are growing increasingly concerned that the economic crisis, which has significantly reduced demand for Chinese exports and played a major role in the collapse of over 68,000 small Chinese companies, will leave millions of workers unemployed and lead to widespread domestic unrest.[104]

As the situation worsens, the pressure for Huawei and other MNCs to gain a competitive edge over U.S. and European competitors grows. Huawei's CEO called on his employees in July to prepare "psychologically" for the impending downturn; employees must work in "crisis mode" to ensure growth and innovation.[105] The pressure of working for Huawei is well-known in China, and employee depression and suicides have been on the rise this year, according to Chinese press reports. A Huawei employee, speaking on condition of anonymity, said that overtime is part of employee evaluations and the corporate culture encourages overtime to shorten product cycles and remain competitive vis-à-vis international giants.[106]

Huawei and some other large Chinese companies view the crisis as an opportunity to invest in the United States and acquire Western IP at an excellent value.[107] Recent press reports, for example, suggest Huawei will continue to expand in the U.S. market in 2009.[108] China Mobile Ltd. also intends to set up its first R&D center outside of China (in California's Silicon Valley in 2009) to assist its work on Internet and telecommunications integration. Donald Straszheim, an economist and vice chair of Roth Capital Partners, which has handled the financing of Chinese companies, states: "In the global recession, Chinese companies are looking around the world to acquire knowledge."[109] Chinese employees of Frog Design, a consulting firm that develops innovative products for Fortune 500 companies, take the following view of the crisis:

> In China, the rule of the game is always "Stay One Step Ahead of Your Competitors"...[W]hen Chinese businesses run out of initiatives in which to invest their capital or when their investments stop...they make a concerted effort to...invest in research and development. In fact, senior executives in some companies have said publicly that in the near future they would either invest in

> their own health and personal happiness, or they would increase R&D budgets in their businesses to invest in better products to prepare for a new run when the downturn ends...This puts a premium on vision and strategic planning instead of short-term financial risk taking.[110]

Some companies, which lack funds for R&D because of the credit crunch, may simply decide to engage in IP theft to maintain an edge over competitors. Michael Kump, a lawyer specializing in IP law, contends:

> As economic conditions tighten and people start looking for ways to cut corners and gain an advantage, some will cross the line...in an illegal manner. One of the classic shortcuts is to steal competitors' intellectual property. It can be quicker to target key employees at a successful competitor and try to get those employees to come over to your side than to invest in process and grow your business the right way.[111]

PriceWaterhouseCoopers notes that established Chinese companies can greatly benefit from employee IP transfer; former U.S. technical specialists can receive financial support to establish start-up companies that rely on the proprietary knowledge obtained from their U.S. employers.[112]

As the global economy continues to weaken, Chinese corporations will likely seek to expand their CI and R&D activities in the United States to increase productivity and improve their competitive positions. This growth will include acquiring struggling U.S. technology firms or their R&D centers, which could result in windfall IP transfers to Chinese firms. Jin Chen, a professor at Zhejiang University, asserts that Holly, a Chinese conglomerate, used its wholly-owned subsidiary in the U.S. to identify and acquire the Code-Division Multiple Access R&D unit from Phillips Electronics, which gave Holly rights to all IP at the facilities and many experienced engineers. The acquisition allowed Holly to improve its mobile telephone chip designs and position in the Chinese telecommunications market.[113] Other notable examples include Lenovo's purchase of IBM's personal-computer business, the Shanghai Automotive Industry Corporation acquisition of Rover technology to create the Roewe brand,[114] and Huawei's purchase of Marconi to tap European markets and relationships with local carriers.[115]

The list of high technology companies that are reducing their technical staff is growing. Sun Microsystems Inc. announced in early November 2008 that it would lay off about 6,000 employees. Teradyne Inc., the leading maker of microchip test equipment, stated it would release about 185 workers worldwide. National Semiconductor Corp., which makes chips, decided to lay off 330 employees and Applied Materials Inc., a manufacturer of chip equipment, announced it would cut 1,800 positions.[116] Some Chinese companies may increase efforts to hire recently laid-off employees of U.S. high technology firms, which could be a growing source of IP transfer.[117]

RECOMMENDATIONS

The following recommendations are provided for the consideration of the U.S. government:

Take Steps to Encourage the Chinese Government and Industry to Stop Illegal Industrial Espionage and Large-Scale Intellectual Property Theft

Thus far, complaints from the U.S. government and industry to stop this illegal behavior have either been met with Chinese government denials, abject disregard, or half-hearted enforcement efforts. Although U.S.-China trade agreements have had some success in curbing IP infringement, U.S. IP industries claim Chinese IP infringement is still occurring at unacceptable levels. It would be neither fair nor accurate to attribute all industrial espionage and IP misappropriation to the Chinese government, or state that all Chinese firms are engaged in this sort of behavior. However, the mounting evidence of Chinese illegal activities is creating a dark cloud of mistrust regarding Chinese business practices that fuels the more pessimistic views of Beijing's plans and intentions.

U.S. government representatives should impress upon their Chinese counterparts that this behavior could have a long-term negative impact on U.S. public perception of China. In addition, given the level of Chinese industrial espionage, the U.S. government should consider enacting laws that would impose more severe sanctions on Chinese companies whose employees are caught stealing U.S. technology and IP.

Closely Review Proposals of Chinese Companies to Purchase R&D Centers of U.S. High-Technology Companies

Huawei proposed to purchase its U.S. competitor 3Com last year, which would have given it access to technology supplied to the Pentagon.[118] Although this was clearly a case in which national security interests were at stake, a closer examination of future high-technology purchase proposals may reveal security implications that are not quite so obvious.

Make CI a New Strategic Theme in the IC

The IC should consider designating CI as a new 'strategic research theme' to help identify and monitor new trends in foreign intelligence that could impact homeland security.[119] China has made CI the center of its intelligence studies and, as mentioned, this is having an impact on Chinese government intelligence research. CI exerts an important influence on the evolution of intelligence programs in other countries as well. In France, for example, CI "involves all levels of government, numerous support organizations from the private and public sectors as well as public private partnerships and quasi-governmental organizations, like the Chamber of Commerce and Industry...or the Agency for the Diffusion of Information and Technology."[120]

Develop Programs on IP and CI at U.S. Government Civilian and Military Colleges and Universities

The extensive Chinese literature on CI has provided a window into a side of China that one is otherwise hard-pressed to find: a detailed discussion of Chinese government intelligence and counterintelligence operations. CI gave the Chinese a vehicle through which they could once again openly discuss intelligence and operations within the politically safe context of international business. At the same time, U.S. literature and understanding on the subject is relatively inadequate, with few books having been written on the subject of Chinese intelligence operations. Against this backdrop, the U.S. government should develop courses and sub-discipline programs at government civilian

and military colleges and universities to train and educate students and professionals in IP and CI matters.

Devote More Funding to Collection and Analysis

As part of this effort, the IC should devote more resources and funding to collection and analysis of the Chinese S&T and IP collection issues. As S&T intelligence requirements are part of the NIPF (National Intelligence Priorities Requirements Framework), according to the RAND report IP requirements should be combined with S&T requirements and ranked among the 'hottest priorities.' The IC should also require Chinese S&T analysts to obtain a deeper understanding IP issues and the development of Chinese language skills. S&T analysts who do not have S&T backgrounds should be required to obtain formal training and education in critical S&T areas.

The IC also needs more intelligence officers to devote to the problem. Despite the rapid increase in cyber security incidents and illegal technology transfer activities in America, the number of officers available to handle these cases remains limited. For example, the number of FBI agents assigned to handle Chinese spying activities in the United States has only risen from 150 in 2001 to 350 in 2007.[121]

Develop a Cadre of Analysts, Scientists, and Technical Personnel with Chinese Language Proficiency

The IC also requires more S&T analysts fluent in Chinese. As suggested in some of the declassified National Intelligence Estimates (NIE) on China (from 1949 to 1976), the IC had difficulty assessing the strategic objectives, military, and scientific and technical capabilities of China because the IC lacked collection in some areas and was forced to rely on Chinese press reporting.[122] Given China's intense secrecy today, IC China analysts are perhaps forced to rely on Chinese open source material more than analysts focusing on other foreign countries. [123]

Unfortunately, only a limited number of IC analysts can read Chinese; translating scientific and technical Chinese documents requires specialized skill. More China analysts must develop the capability to read and understand scientific and technical Chinese. Developing this skill is especially crucial for today's S&T analysts because of the great strides China is making in S&T and R&D (many key Chinese S&T documents and books have only been published in Chinese).

The following recommendations are provided for the consideration of U.S. corporations:

Establish or Strengthen Competitive Intelligence Programs

U.S. corporate executives and managers also need to develop or strengthen intelligence and counterintelligence programs in their companies. Some Chinese companies are outperforming their U.S. competitors in this area, and their successes can provide useful lessons for U.S. companies doing business with China. The consensus in the Chinese literature on CI is that training and education is essential for a successful CI program.[124] Although U.S. companies also understand this is important, they lag far behind some Chinese companies in CI training and education. For example, while DuPont employees are required to complete online training regarding insider risks,[125] employees in some Chinese companies are obtaining their doctorates in CI.[126]

Consider Sending Employees to Outside Competitive Intelligence Training Courses

Company employees could learn a great deal about CI matters by attending outside CI training courses in China and the United States. Chinese companies send employees to CI courses held in various cities in China. The Chinese Business Training Network (CBTN) offers CI courses in China almost monthly. The course syllabus covers the following selected topics: goals of intelligence and competitive intelligence collection; using intelligence analysis and production methods; preventing disclosure of proprietary information during company visits; developing insiders in competitors' companies; creation of social networks to find and recruit key IT personnel; creating CI units within the company; establishing clear lines of communication and support with other departments; protecting trade secrets; identifying and neutralizing intelligence threats; and case studies on real espionage cases and lessons learned (including case studies based on traditional CIA espionage operations and Chinese corporate counterintelligence investigations).[127]

Increase Collaboration with Government Agencies and Heed Government Warnings

Although the FBI and DHS have set up official groups within which U.S. companies can confidentially reveal their computer network vulnerabilities to the government,[128] some companies remain loath to do so, for reasons mentioned previously. The *National Journal's* recent article on Chinese hacking also suggests that some U.S. companies view government warnings as alarmist hyperbole.[129]

Strengthen Protection of Sensitive Data and Consider the Long-term Risks Associated with Lay-Offs of Employees with Knowledge of Critical Proprietary Information

As high-technology corporations increase employee lay-offs, they must take steps to ensure their sensitive data is well protected. Current information storage technologies, such as USB drives and other devices, have facilitated the ability of employees to take vast amounts of proprietary information to a company's competitors.[130] Cadence Design Systems, a software company, developed standard operating procedures – consisting of strict access and document controls, enterprise rights management and compartmentalization – to control the unauthorized release of such proprietary information. Cadence also employs modular software development procedures to compartmentalize information when conducting R&D in developing countries.[131] However, the potential problem with such a method is that all of the money and effort put into its design can be lost if only one trusted employee with access to the right proprietary data departs the company and works for a competitor. Many U.S. high-technology corporations, with the sole aim of cutting costs, often release employees without even assessing how they could damage compartmentalization efforts and long-term market position.

CONCLUSION

The U.S.-China Economic Security and Review Commission warns in its 2007 annual report that, as U.S. companies continue to develop new technologies in hundreds of high-tech factories and joint R&D facilities in China, Chinese espionage poses the most significant threat to U.S. technology. If the U.S. government and industry cannot adequately control Chinese espionage in America, they certainly cannot expect to stop massive IP infringement and theft from U.S. R&D centers and other facilities located in China. Although U.S. IP industries can continue to push for stronger legislation (in both America and China) that would increase the penalties for Chinese companies and individuals involved in espionage, they must take steps to protect their intangible property to maintain their competitive positions worldwide.

China's large-scale infringement and theft of IP hurts the U.S. economy and, at the same time, helps advance Chinese science and technology, improve new weapons systems, and develop new products and processes. If America cannot do better at curbing these activities, then it becomes imperative for the IC to develop more robust methods of following Chinese S&T developments and informing policymakers of their potential ramifications. As U.S. preeminence in S&T and IP begins to wane, the importance of tracking and understanding emerging trends – such as CI in China – grows. Left unchecked, Chinese illegal forms of intelligence collection will enhance China's corporate intelligence programs and competitive advantage to the detriment of U.S. corporations and the U.S. economy.

China must strengthen efforts to cooperate with the United States on stopping such illegal activities, which greatly damage China's image and could push American public opinion toward protectionism or economic retaliation during an extended economic downturn.[132] As the cases of contaminated Chinese food products and toys demonstrate, the short term economic benefits of unscrupulous and illegal behavior is not worth the long-term damage to the image of Chinese corporations and their business practices in the United States. The majority of ethical Chinese businessmen and laborers have worked too hard over the last several decades to watch their many successes become tarnished by the refusal of the Chinese government and unscrupulous corporations to admit and stop such wrongdoing.

Robert Slate is a lead systems engineer at the MITRE Corporation. He formerly served as a captain in the U.S. Army and faculty member at the National Defense Intelligence College, Post-Graduate Intelligence Program-Reserves. Prior to obtaining his Juris Doctorate, he received his master's degree from the Fletcher School of Law and Diplomacy and bachelor's from Oberlin College. Slate is currently pursuing his PhD in environmental science. He has previously published articles on U.S. intelligence and Chinese military, strategy, and legal issues. Mr. Slate may be contacted at rbslate@gmail.edu.

[†] The views express in this manuscript are the author's and do not reflect the official position of the MITRE Corporation or imply endorsement by the Office of the Director of National Intelligence or any other U.S. government agency. The author's affiliation with MITRE is provided for identification only. It does not convey or imply MITRE's concurrence with, or support for, his positions, opinions, or viewpoints.

[1]China Business Training Network (CBTN), *Competitive Intelligence Gathering and Trade Secret Protection Practices* (Shanghai, China, 2008), http://hk.top.sh/main/detail.net?IDTradeInfo=21554. [Hereafter cited as *Trade Secret Protection.*]

[2] "Competition from China: Two McKinsey Surveys," *The McKinsey Quarterly* (2008): 8. [Hereafter cited as "Two Mckinsey Surveys"]; The National Counterintelligence Executive's 2005 report holds: "Foreign governments and intelligence organizations have created quasi-official organizations to enable them to capitalize on the private-sector technology theft that is underway. Indeed, the CI Community believes that foreign governments are major beneficiaries of the private-sector technology flow...To elicit sensitive information from those attending these quasi-official organizations, government officials may appeal to the professional egos of the private sector contacts, to their patriotism, or to their commercial sensibilities, by offering domestic business deals to accomplish technology transfer. Coercion is also an option in countries like Russia and China, where security services still hold considerable sway over the private sector." National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2005)*, (Washington, DC: National Counterintelligence Executive, 2006), 6. [Hereafter cited as *Collection and Industrial Espionage.*]

[3] The Office of the Director of National Intelligence (DNI) states human intelligence collection "is performed by overt collectors such as diplomats and military attaches... [and] includes clandestine acquisition of photography, documents, and other material; overt collection by personnel in diplomatic and consular posts; debriefing of foreign nationals and U.S. citizens who travel abroad; and official contacts with foreign governments." See Official Website, Office of the Director of National Intelligence, http://www.dni.gov/what_collection.htm.

[4] Wesley Wark suggests some methods of technical collection, such as "line-tapping, bugging, outputs from remote sensors, computer hacking (and) perhaps 'deep mining' of the Internet" can be difficult to neatly place in any single-intelligence agency category. Wesley Wark, *Twenty-First Century Intelligence* (Oxford, UK: Routledge, 2005), 53. Technical collection generally refers to signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT) and geospatial intelligence (GEOINT). According to the DNI, SIGINT "is derived from signal intercepts comprising – however transmitted – either individually or in combination: all communications intelligence (COMINT); electronic intelligence (ELINT); (and) foreign instrumentation (FISINT). Ibid. For the purposes of this paper, "illegal" technical collection primarily refers to illegal SIGINT and computer hacking.

[5] Joby Warrick and Carrie Johnson, "Chinese Spy 'Slept' in U.S. for 2 Decades," *The Washington Post*, April 3, 2008. [Hereafter cited as *Decades.*]

[6] See, for example, Wang Qi, "Business Competition and Competitive Intelligence," [*Qiye Jingzheng yu Jingzheng Qingbao*] *Military Dual-Use Technology and Products* (2002); "A Chinese Website advertising a technology exhibit in April 2006 in Chongqing, China, highlights the emphasis Beijing places on facilitating the transfer of technology from civil to military uses. According to the Website, the exhibit has three objectives: breaking down the barriers to sharing technology among industries, bureaucratic entities, and state and private sectors; facilitating coordinated development between the civilian hi-tech sector and the military; serving as a technology-exchange platform for civilian and military technologies." *Collection and Industrial Espionage, supra* note 2, 5.

[7] Christopher Bellavita, in his article "Changing Homeland Security: Shape Patterns, Not Programs," *Homeland Security Affairs* II, No.3 (October 2006), notes the majority of homeland security policy matters are overly "undefined...broad...(and) complex." [Hereafter cited as *Shape Patterns.*]

[8] Li Yingzhou et al., *A Summary of Nearly a Decade of Competitive Intelligence Research in China* [*Jin Shi Nian Wo Guo Jingzheng Qingbao Yanjiu Zengshu*] (Jan. 1, 2007) http://www.zoomchina.cn/content/view/45/97/1_0.html. [Hereafter cited as *Decade of CI.*]

[9] Jamie Smith and Leila Kossou, "The Emergence and Uniqueness of Competitive Intelligence in France," *Journal of Competitive Intelligence and Management*, No. 4.3 (2008): 65. [Hereafter cited as *CI in France.*]

[10] Loius Le Comte, *Memoirs and Observations Typographical, Physical, Mathematical, Mechanical, Natural, Civil, and Ecclesiastical, Made in a Late Journey through the Empire of China, and Published in Several Letters*, Printed for Benj. Tooke at the Middle Temple Gate, and Sam. Buckley at the Dolphin over against St. Dunstans Church in Fleetstreet (London, 1697), 238-239. [Hereafter cited as *Memoirs*.]

[11] Over the past sixteen years, foreign direct investment in China has reached almost a half-trillion dollars; China's annual economic growth rate has routinely topped upwards of 8 percent, and some years it has approached 10 percent. David Lei, "Outsourcing and China's Rising Economic Power," *Orbis: A Journal of World Affairs* 51, No. 1 (2007).

[12] See, for example, David D. Hale and Lyric Hughes Hale, "Reconsidering Revaluation: The Wrong Approach to the U.S.-Chinese Trade Imbalance," *Foreign Affairs* (Jan/Feb 2008): 57; Felix K. Chang and Jonathan Goldman, "Deterring the Debt Weapon," *The American Interest* 3, No. 5 (May/June 2008): 86-87.

[13] *Global Intangible Tracker 2006: An Annual Review of the World's Intangible Value* (December 2006), http://www.brandfinance.com/Uploads/pdfs/Global%20Intangible%20Tracker%202006.pdf.

[14] *Global Intangible Tracker 2007: An Annual Review of the World's Intangible Value* (December 2007), http://www.brandfinance.com/Uploads/pdfs/BF_GIT_07_REPORT_Final%20Version%20Low%20Res.pdf.

[15] *The Invisible Business*, http://www.brandfinance.com/Uploads/pdfs/Invisible%20business.pdf.

[16] Robert Slate, "China's National Intellectual Property Strategy: Implications for U.S. National Security," *Defense Intelligence Journal* 16, No. 2 (2007): 31. [Hereafter cited as *Implications*.]

[17] "IIPA's New Economic Study Reveals the Copyright Industries Remain a Driving Force in the U.S. Economy," January 30, 2007, http://www.iipa.com/pdf/IIPA2006CopyrightIndustriesReportPressReleaseFINAL01292007.pdf.

[18] See *Memoirs*, supra note 10, 238-239.

[19] Ibid., 238.

[20] *Redefining Intellectual Property Value: The Case of China* (PriceWaterhouseCoopers, 2005), 31. [Hereafter cited as *Case of China*.]

[21] Ibid.

[22] "FBI: China May Use Counterfeit Cisco Routers to Penetrate U.S. Networks," *WorldTribune.com*, May 15, 2008, http://www.worldtribune.com/worldtribune/WTAR/2008/ea_china0141_05_15.asp. See also, Brian Grow, et al., "Dangerous Fakes: How Counterfeit, Defective Computer Components from China are Getting into U.S. Warplanes and Ships," *Business Week*, October 13, 2008, 036. [Hereafter cited as *Dangerous Fakes*.]

[23] Ibid.

[24] *Dangerous Fakes, supra* note 22, p. 035.

[25] *Decades, supra* note 5.

[26] Brian Grow, Keith Epstein, and Chi-Chu Tschang, "The New E-Spionage Threat: A BusinessWeek Probe of Rising Attacks on America's Most Sensitive Computer Networks Uncovers Startling Security Gaps," *Business Week*, April 21, 2008, p. 034. [Hereafter cited as *E-Spionage*.]

[27] Ibid., 035.

[28] Ibid., p. 033.

[29] According to the *National Journal*, the Chinese government and military employs computer hackers to steal government secrets and corporate proprietary information. Shane Harris, "China's Cyber-Militia:

Chinese Hackers Pose a Clear and Present Danger to U.S. Government and Private-Sector Computer Networks and May Be Responsible for Two Major U.S. Power Blackouts," *National Journal Magazine* 31 (May 2008), http://www.nationaljournal.com/njmagazine/print_friendly.php?ID=cs_20080531_6948. [Hereafter cited as *Cyber-Militia.*]

[30] *E-spionage, supra* note 26, 040.

[31] *Case of China, supra* note 20.

[32] *Implications, supra* note 16, 43-48.

[33] David J. Lynch, "FBI Goes on Offensive Against China's Tech Spies," *USA Today*, July 7, 2007, http://www.usatoday.com/money/world/2007-07-23-china-spy-2_N.htm. [Hereafter cited as *FBI Offensive.*]

[34] Craig Covault and James Ott, "Caught in the Net: Justice Dept. Implicates Iran, China Contacts in Tech-Transfer Violations," *Aviation Week & Space Technology*, November 3, 2008, 34.

[35] Ibid. See also, Department of Justice, *Chinese National Sentenced for Economic* Espionage (2008), http://hongkong.usconsulate.gov/uscn_others_20080618o2.html.

[36]Zheng Chengsi, *Shortcomings of the Information, Intellectual Property and the Intellectual Property Strategy of China* [*Xinxi, Zhishi Chanquan yu Zhongguo Zhishi Chanquan Zhanlue Ruogan Wenti*] (January 20007), http://www.sipo.gov.cn/sipo/xwdt/mtji/2007/200701/t20070129_131223.htm; Lin Yuhong, *Zheng Chengsi: Guobao Ji* [Zheng Chengsi: National Treasure] *Guangming Daily*, September 17, 2006, http://www.gmw.cn/01gmrb/2006-09/17/content_480949.htm; See also, *Implications, supra* note 16, 42

[37] *Implications, supra* note 16, 42; State Council of the People's Republic of China, *Outline of the National Intellectual Property Strategy*, §V (1)(40) (June 5, 2008), available at http://www.law-now.com/law-now/sys/getpdf.htm?pdf=outlincof thenationalintellectualpropertystrategy1.pdf. [Hereafter cited as *Strategy.*] The impetus for the IP strategy largely originated from the tireless efforts of the late Professor Zheng Chengsi, the "father of IP in China" and former director of the IP Office of the Chinese Academy of Sciences (CAS). Zheng visited Japan's Patent Office in 2002 to learn more about Japan's newly-launched National IP Strategy. Japan's IP Strategy impressed Zheng because Japan had used it to help revitalize its lagging economy. Subsequently, Zheng held a large-scale seminar on Japan's IP Strategy at CAS, which became of the substance of a CAS report delivered to the State Council. The report had a significant impact on the Council, and in January 2005, the Council established the Leading Group (LG) for National Intellectual Property Strategy Formulation.

[38] "The administration of intellectual property needs to cover all links in national defense, including research, production, operation, equipment procurement and guarantee, and project management, and control of major intellectual property related to national defense should be strengthened. A guideline to key technologies needs to be published. Create a number of the self-relied intellectual property in areas such as key technologies for weapons and military equipment and high technologies for both military and civilian purposes. An early warning mechanism for intellectual property related to national defense needs to be established, and special examinations of IPRs related to national defense should be carried out in military technology cooperation and arms trade...Make more effective use of intellectual property related to national defense. The rules for keeping secrecy and declassification of intellectual property related to national defense need to be further improved. Promote the use of intellectual property related to the national defense for civilian purposes with the condition that national security and the interests of national defense are not compromised. Encourage the use intellectual property for civilian purposes in the area of national defense." Ibid., §IV (7) (38, 39).

[39] China's push to create standards for third-generation (3G) mobile telephony, based on the TD-SCDMA (Time Division-Synchronous Code Division Multiple Access) standard, and the Internet (IPV6), is motivated by a desire to avoid licensing fees and ground the standards for these technologies in Chinese IP. James Popkin and Partha Iyengar suggest China is generally developing standards to protect domestic firms from foreign competition and, in the case of security standards for wireless communications, to

decrypt and monitor foreign communications inside China. James M. Popkin and Partha Iyengar, *IT and the East: How China and India are Altering the Future of Technology and Innovation* (Boston, MA: Harvard Business School Press, 2007), 24.

[40] Ibid., §VI (1) (30); See also Richard P. Suttmeier et al., *Standards of Power? Technology, Institutions, and Politics in the Development of China's National Standards Strategy* (Seattle, WA: The National Bureau of Asian Research, 2006), 1.

[41] Chien-Hsun Chen et al., *High-tech Industries in China* (Cheltenham, UK: Edward Elgar Publishing, 2005), xv. "In the vast majority of cases, multinationals are willing to provide their China subsidiaries with advanced technology; this was true of 86.6 percent of the multinationals included in the sample. 65.3 percent of the multinationals in the survey were providing technology that had not previously been available in China. Technology obtained from foreign-invested enterprises accounts for over 50 percent of all foreign technology introduced into China; in more than 60 percent of cases multinationals' Chinese subsidiaries are using technology that is less than three years old." Ibid.

[42] Kathleen Walsh, *Foreign High-tech R&D in China: Risks, Rewards, and Implications for US-China Relations* (Washington, D.C.: The Henry L. Stimson Center, 2003), 105.

[43] Ibid.

[44] "2008 Global R&D Report: Changes in the R&D Community," *R&D Magazine*, September 7, 2007, G3, http://www.rdmag.com/pdf/RD79GlobalReport.pdf.

[45] Ibid. See also Maximilian von Zedtwitz, "Managing Foreign R&D Laboratories in China," *R&D Management* 34, No. 4 (2004): 439.

[46] Nannan Lundin and Sylvia Schwaag Serger, *Globalization of R&D and China: Empirical Observations and Policy Implications*, (Stockholm, Sweden: Research Institute of Industrial Economics, 2007), 1.

[47] See *Case of China, supra* note 20, 3-4.

[48] Ibid., 2.

[49] Julian Goldsmith, "Huawei Touts R&D Prowess," *Silicon.com*, September 6, 2007 [hereafter cited as *Prowess*]; Huawei spends approximately 10 percent of its yearly revenue on R&D. See Huaichuan Rui and George S. Yip, "Foreign Acquisitions by Chinese Firms: A Strategic Intent Perspective," *Journal of World Business* (2008), 9. [Hereafter cited as *Strategic Intent*.]

[50] Some Chinese counterfeiting operations are so advanced that they include well-funded and elaborate underground R&D programs. Xu Chao, "Black Phone Innovations [Hei Shouji Chuangxin]," *World Communications Weekly* (June 10, 2008) http://www.cww.net.cn/mobile/html/2008/6/10/20086101826494773.htm; See also *Case of China, supra* note 20, 3-4.

[51] China's IP Strategy is intended to transform China's IP activities from being primarily a legal and trade-related issue, to becoming a strategic imperative that is the domain of Chinese corporations and government agencies. Numerous policymakers and officials from the State Council, SIPO, COSTIND (State Commission on Science, Technology and Industry for National Defense), the Ministry of Science & Technology (MOST), CAS, Supreme People's Court (SPC), Ministry of Public Security (MPS) and representatives from top universities in China, such as Beijing and Qinghua Universities, have been involved in developing, collaborating and coordinating on various aspects of the Strategy. Coinciding with the development of the IP Strategy, statements on the importance of IP and the IP Strategy for improving the development of the national economy, innovation and military weaponry began to appear in national S&T development plans, China's National Defense White Papers (NDWP) (2006), and COSTIND publications—a relatively recent phenomenon in China. The NDWP, for example, emphasizes that the military should improve innovation to build better weapons and equipment and that increased R&D in the military has resulted in the development of new S&T inventions and IP. *Implications, supra* note 16, 29.

[52] Li Yan et al., "Analysis of the State of Competitive Technical Intelligence" ["Jishu Jingzheng Qingbaode Xiankuang Fenxi"], *Competitive Intelligence Journal* [*Jingzheng Xuebao*] (2006).

[53] Xue Yafang, *The Growing Demand for Intelligence Personnel Is Becoming More Conspicuous* [*Qingbao Rencai Xuqiu Riyi Xian Xinghua*], April 16, 2005, http://www.chinahrd.net/zhi_sk/jt_page.asp?articleid=76116; Justin L. Bloom, "Japan as a Model for a National Approach to Business Intelligence," W. Bradford Ashton and Richard A. Klavans, eds., *Keeping Abreast of Science and Technology: Technical Intelligence for Business* (Columbus, OH: Batelle Press, 1997), 49.

[54] TRS conducts R&D on information retrieval and content management systems for the Chinese government and industry and provides information technology support to corporate and government CI systems. TRS Website [[in Chinese], *Company Profile,* http://www.trs.com.cn/company/compintro/lhz.

[55] Zhong Tianwei, "The Practice of Competitive Intelligence and Development," 13th Annual Session on China's Competitive Intelligence, Nanning, Guangxi, November 8, 2007, http:www.trs.com.cn/news/ztbd/2007CIS/.

[56] W. Bradford Ashton and Richard A. Klavans, "An Introduction to Technical Intelligence in Business," *Keeping Abreast of Science and Technology: Technical Intelligence for Business* (Columbus, OH: Battelle Press, 1997), 113-114. [Hereafter cited *Technical Intelligence.*]

[57] Justin L. Bloom, "Japan as a Model for a National Approach to Business Intelligence," 49.

[58] See Chinese SCIP Official Website, http://www.scic.org.cn/NOTICE/08lj.doc.

[59] *Decade of CI*, *supra* note 8.

[60] Chen Feng, *Mian Xiang Qiye Zhanlue Guanli de Jingzheng Qingbao* Yanjiu [Research on Competitive Intelligence and Strategic Management], Ph.D. Dissertation, Beijing University (2002) [hereafter cited as *CI & Strategic Management*]; Liu Ting, *Guojia Anquan de Qingbao Baozhang Tixi Yanjiu* [Research on Intelligence Support to National Security], Ph.D. Dissertation, Nanjing University (2002).

[61] See for example, http://www.dinglv.com.cn/zjtd.html.

[62] CTI techniques could include technology prospecting, Web mining, data mining, patent analysis or scientometrics, etc.; W. Bradford Ashton and Richard A. Klavans, "An Introduction to Technical Intelligence in Business," *Keeping Abreast of Science and Technology: Technical Intelligence for Business* (Columbus, OH: Battelle Press, 1997), 11. [Hereafter cited *Technical Intelligence.*]

[63] *Decade of CI*, *supra* note 8.

[64] Ibid.

[65] *Cyber-Militia*, *supra* note 29.

[66]Chinese R&D and CI labor costs are significantly lower than in America. According to Huawei, at one-fifth of that in the West, Chinese multinational giants can compete in the R&D arena with less than a quarter of the R&D budget of large Western firms. *Prowess*, *supra* note 49.

[67] *Technical Intelligence*, *supra* note 56.

[68] See *Decade of CI*, *supra* note 8.

[69] Chinese companies that are located in high-tech science parks in China not only benefit from preferential tax, financial and foreign exchange treatment, but are also able to collaborate with first-class research institutes and universities. Beijing's Zhongguancun Science Park, for example, contains over 12,000 firms and is located in the Haidian district, which contains 232 scientific research institutes, 73 universities (including the Harvard and MIT of China, Beijing University and Qinghua University, respectively). Company R&D and innovation costs are tax deductible, and imported technology and IP receive tariff exemptions. According to official Chinese data, the park's gross industrial output reached about $25 billion in 2003. Quanlin Gu et al., "Firm Dynamics in Economic Transition: Evidence from a

Chinese Science Park," in Haiying Li, ed., *Growth of New Technology Ventures in China's Market* (Cheltenham, UK: 2006), 35.

[70] Notra Trulock, the former director of intelligence at the U.S. Department of Energy, writes: "[T]he Chinese approached spying differently from the Russians... Chinese techniques were "nontraditional" in that they concentrated more on eliciting information from visiting scientists and other officials and less on Soviet-style spycraft...[T]he Chinese would employ scientists, academicians and students to collect information of interest...Intelligence taskings would come from scientists or academic institutions engaged in research for the People's Liberation Army or from other government customers...The Chinese painstakingly collected lab and Energy Department unclassified technical reports, and visitors to Chinese facilities were struck by the thoroughness of their collections. In their own writings, the Chinese assessed these reports as 'provid[ing] intelligence of great value.' The Chinese knew all about the labs' penchant for sloppy handling and "inadvertent" releases of classified documents..." Notra Trulock, *Code Name Kindred Spirit: Inside the Chinese Nuclear Espionage Scandal* (San Francisco, CA: Encounter Books, 2003), 106-07; Chinese companies located in the park also have access to government-supported research in scientific and technical areas. *Strategic Intent, supra* note 49, 5.

[71] Some large Chinese companies receive financial support from the Chinese government for some of their illegal activities, and in turn, assist the military or civilian intelligence services with identifying and acquiring foreign technology. *The Cox Report: U.S. National Security and Military/Commercial Concerns with the People's Republic of China*, Report of the Select Committee, United States House of Representatives (Washington, DC: Regnery Publishing, Inc., 1999), 68-70. [Hereafter cited as *Cox Report.*]

[72] *Cyber-Militia, supra* note 29.

[73] *E-spionage, supra* note 26, 040.

[74] *Cox Report, supra* note 72.

[75] Roger Z. George, "Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm," *Studies in Intelligence* 51, No. 3 (Extracts-September 2007): 1, citing Director of National Intelligence, *Report on the Progress of the Director of National Intelligence in Implementing the "Intelligence Reform and Terrorism Prevention Act of 2004,"* May 2006, 5-11. Available online at http://www.dni.gov/reports/CDA_14-25-2004_report.pdf.

[76] Ibid.

[77] *Cox Report, supra* note 72, p. 87.

[78] Ibid., 87-88.

[79] Ibid., 88.

[80] Ibid.

[81] Ibid..

[82] Robert M. Clark, "Scientific and Technical Intelligence Analysis," *Studies in Intelligence*, 19, No. 1 (Spring 1975), in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal*, 1955-1992 (New Haven, CT: Yale University Press, 1995), 294. [Hereafter cited as *Intelligence Analysis.*]

[83] *CI & Strategic Management, supra* note 60.

[84] Rob Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, 2005), 66-70. [Hereafter cited as *Analytic Culture.*]

[85] Ibid.

[86] Ibid., 67.

[87] Gregory F. Treverton and C. Bryan Gabbard, *Assessing the Tradecraft of Intelligence Analysis* (Santa Monica, CA: RAND Corporation, 2008), 4. [Hereafter cited as *RAND report.*]

[88] *Intelligence Analysis*, *supra* note 82, 294.

[89] *Cox Report*, *supra* note 72, 50.

[90] *Analytic Culture*, *supra* note 84, 66-70.

[91] *RAND report*, *supra* note 87, 1.

[92] Ibid.

[93] Ibid., 48.

[94] Ibid., 7.

[95] *Decades*, *supra* note 5, A1.

[96] *Cyber-Militia*, *supra* note 29.

[97] *Two McKinsey Surveys*, *supra* note 2, 6.

[98] Curtis R. Carlson and William W. Wilmot, *Innovation: The Five Disciplines for Creating What Customers Want* (New York, NY: Crown Publishing Group, 2006), 268-269. [Hereafter cited as *Innovation.]*

[99]" Revving Up: How Globalization and Information Technology are Spurring Faster Innovations, in Special Report on Innovation," *Economist*, October 13, 2007, 6.

[100] *Implications*, *supra* note 16, 46.

[101] *Innovation*, *supra* note 98, 268-269.

[102] Geoffrey Colvin, "America Isn't Ready: Here's What to Do About It," *Fortune*, August 4, 2005, 77.

[103] *Chinese Leader Says China Losing Competitive Edge* (November 30, 2008), http://news.yahoo.com/s/ap/20081130/ap_on_bi_ge/as_china_economy.

[104] Ariana Eunjung Cha, "As China's Losses Mount, Confidence Turns to Fear Officials Use Bailouts to Forestall Unrest," *Washington Post Foreign Service*, November 4, 2008, A01.

[105] Robert Clark, *Huawei Posts Record Result, Frets About Downturn* (July 14, 2008) http://www.telecomasia.net/article.php?id_article=9446.

[106] According to various reports, Huawei encourages a "mattress culture" where every software developer keeps a mattress in the office to sleep after hours. "Huawei CEO Writes a Letter to Employees Addressing the Issue of Depression" [Huawei CEO Gei Yuangong Xie Yantan Yindu Zao Bao Guang] *Daily Economic News* [*Meiri Jingji Xinwen*], April 18, 2008, http://news.xinhuanet.com/employment/2008-04/18/content_8002142_1.htm.

[107] Tim Lebrecht, "For China, the Financial Crisis is An Opportunity," *CNET Blog Network*, October 18, 2008, http://news.cnet.com/8301-13641_3-10069536-44.html.

[108] "Huawei's Ever-Expansion Strategy May Hit a Wall, or Not," October 31, 2008, http://www.chinastakes.com/story.aspx?id=781.

[109] James Flanigan, "An Eye on Growth, Deals Stretch Across the Pacific," *New York Times*, November 20, 2008, http://www.nytimes.com/2008/11/20/business/smallbusiness/20edge.html.

[110] Ibid.

[111] Meridith Levinson, "How to Avoid Getting Sued by a Former Employer," November 13, 2008, http://www.cio.com/article/462663/How_to_Avoid_Getting_Sued_by_a_Former_Employerhttp://www.cio.com/article/462663/How_to_Avoid_Getting_Sued_by_a_Former_Employer.

[112] The company's 2005 study on Chinese IP points out: "In China, a large number of technical specialists who have retired after enjoying a full career in the United States or Europe discover a very supportive

environment for a second career in China...funds are available for such start-ups from domestic and foreign sources, and venture capital money increasingly is attracted to ones with major potential and apparent political support." *Case of China, supra* note 20, 5.

[113] Jin Chen and R. Michael Holmes Jr., "Theory and Empirical Evidence on R&D Globalization in Chinese Firms," in Haiying Li, ed., *Growth of New Technology Ventures in China's Market* (Cheltenham, UK: 2006), 273-74.

[114] Thomas Luedi, "China's Track Record in M&A," *The McKinsey Quarterly*, No. 3 (2008), 77.

[115] *Strategic Intent, supra* note 49, 9.

[116] Hiawatha Bray, "Downturn Lashes into High Tech: Industry Cutting Thousands of Positions as Businesses and Consumers Trim Purchases," *The Boston Globe*, November 15, 2008, http://www.boston.com/business/technology/articles/2008/11/15/downturn_lashes_into_high_tech/.

[117] *Case of China, supra* note 20, 5.

[118] *Implications, supra* note 16, 43.

[119] Christopher Bellavita suggests using a "pattern-based approach" to help make sense of such evolving homeland security issues "to sift through the elements of strategic disorder...and determine whether an issue can be ordered—and thus subject to a rich set of knowledge and methodologies..." See *Shape Patterns, supra* note 7.

[120] *CI in France, supra* note 9, 64.

[121] *FBI Offensive, supra* note 33.

[122] See, for example, National Intelligence Council, *Tracking the Dragon: National Intelligence Estimates on China During the Era of Mao, 1948-1976* (Washington, DC: National Intelligence Council, 2004), 405-412.

[123] Ibid.

[124] *Decade of CI, supra* note 8.

[125] *FBI Offensive, supra* note 33.

[126] *Decade of CI, supra* note 8.

[127] See *Trade Secret Protection, supra* note 1.

[128] *Cyber-Militia, supra* note 29.

[129] Ibid.

[130] "Data Theft Experts Discuss Enforceable Data Leakage Prevention Policies During Economic Downturn," *MarketWire*, November 10, 2008, http://www.marketwatch.com/news/story/Data-Theft-Experts-Discuss-Enforceable/story.aspx?guid=%7BF20E3631-A4FA-4A1F-A391-5ACBD07B472D%7D.

[131] 'You just don't give the developers access to the code tree the way we would in an equivalent position here...We're just opening up Russia as an example. We have 100 people there; we'll have 200 people there a year from now. They're superb engineers. They are the best of the best out of the Russian Academy of Sciences and their engineering schools, and they're astonishing mathematicians. So we're giving them big math problems, big algorithm problems to help drive the heart of these software packages that we produce. It doesn't connect to anything for them—it's just a big matrix to solve, and they're doing a marvelous job of it.'" *Case of China, supra* note 20, 58-60.

[132] Thomas P.M. Barnett, "Ten Reasons Why China Matters To You," *Good* 10 (2008), 63. Although Professor David Lampton, Director of China Studies at John's Hopkins University's School of Advanced International Studies, does not support a "confrontationalist" policy toward China, he concedes that China must cooperate with the United States on the matter of intellectual property protection: "China

simply is too big to be allowed to violate foreign intellectual property the way earlier, smaller modernizing economies did. Beijing has to assume responsibility for the local officials who have become addicted to the revenues and employment their localities generate through the theft of intellectual property." David M. Lampton, "Paradigm Lost: The Demise of "Weak China," *The National Interest*, No. 81 (2005), 79-80.

RELEASE

Department of Justice

FOR IMMEDIATE RELEASE
Tuesday, October 28, 2008
WWW.USDOJ.GOV

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

More Than 145 Defendants Charged in National Export Enforcement Initiative During Past Fiscal Year

Three Charged Today in Plot to Export Sensitive Technology to China Space Entity; New Counter-Proliferation Task Forces & Training Part of National Effort

WASHINGTON -- A multi-agency initiative to combat illegal exports of restricted military and dual-use technology from the United States has resulted in criminal charges against more than 145 defendants in the past fiscal year, with roughly 43 percent of these cases involving munitions or other restricted technology bound for Iran or China, the Justice Department and several partner agencies announced today.

Over the past fiscal year, the National Export Enforcement Initiative has also resulted in the creation of Counter-Proliferation Task Forces in various judicial districts around the country. Today, there are approximately 15 such task forces or versions of them nationwide. In addition, the initiative has resulted in enhanced training for more than 500 agents and prosecutors involved in export control and the creation of new mechanisms to enhance counter-proliferation coordination among law enforcement agencies, export licensing agencies and the Intelligence Community.

Among the most recent cases brought in connection with the initiative was an indictment returned today in the District of Minnesota charging three individuals, Jian Wei Ding, Kok Tong Lim, and Ping Cheng, with conspiring to illegally export to the People's Republic of China (PRC) controlled carbon-fiber material with applications in rockets, satellites, spacecraft, and uranium enrichment process. According to the indictment, the intended destination for some of the material was the China Academy of Space Technology, which oversees research institutes working on spacecraft systems for the PRC.

Unveiled in Oct. 2007, the National Export Enforcement Initiative is a cooperative effort by the Justice Department's National Security Division (NSD), the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE), the Federal Bureau of Investigation (FBI), the Department of Commerce's Bureau of Industry and Security (BIS), the Pentagon's Defense Criminal Investigative Service (DCIS), the State Department's Directorate of Defense Trade Controls, the Treasury Department's Office of Foreign Assets Control and other agencies.

The Threat from Illegal Exports

On a daily basis, foreign states as well as criminal and terrorist groups seek arms, technology, and other materials to advance their technological capacity, weapons systems and, in some cases, Weapons of Mass Destruction programs. With America producing the most advanced technology in the world, it has become a primary target of these illicit technology acquisition efforts. The U.S. government, defense sector, private companies, and research institutions are routinely targeted as sources of these materials.

The items sought from America in these illicit schemes are as diverse as missile technology, nuclear

technology, assault weapons, trade secrets, source code, military aircraft parts, night vision systems, and technical know-how. The improper transfer of these items poses threats to U.S. allies, U.S. troops overseas, and to Americans at home. It also undermines America's strategic, economic, and military position in the world.

"Keeping U.S. weapons technology and other restricted materials from falling into the wrong hands and from being used against our allies, our troops overseas or Americans at home is a top counter-intelligence priority of the Justice Department," said Patrick Rowan, Assistant Attorney General for National Security. "Through this multi-agency initiative we are making America a far more hostile target for those that seek to obtain our sensitive technology through illegal means."

Enhanced Prosecutions and Investigations

In recent years, as investigative agencies have stepped up their efforts to address this threat, the Justice Department has handled a growing number of cases involving illegal exports of sensitive U.S. technology and embargo violations. Last year, the Department decided to institutionalize the expansion of its export control efforts through the launch of the National Export Enforcement Initiative, which is designed to increase training and coordination among agencies involved in export control, enhance prosecution of these crimes, and deter illicit activity.

To implement the initiative, the Justice Department appointed its first National Export Control Coordinator in June 2007. In October 2007, the Department joined forces with counterparts from ICE, FBI, BIS, DCIS, the Department of State and other agencies to publicly announce the initiative. Since that time, the number of prosecutions has continued to grow, as investigative agencies have increased the tempo of their operations and prosecutors have become more familiar with this area of law.

During Fiscal Year (FY) 2008, there were more than 145 defendants charged in export control or embargo cases, compared to roughly 110 charged in FY 2007. There have been more than 255 defendants charged in such cases over the past two fiscal years. Charges brought in these cases include violations of the Arms Export Control Act, the International Emergency Economic Powers Act (IEEPA), the export control provision of the PATRIOT Reauthorization Act, the Trading with the Enemy Act, and other statutes.

Restricted Materials Bound for Iran and China

Roughly 43 percent of the defendants charged in FY 2008 were charged in export control or embargo cases involving Iran or China. In total, Iran ranked as the leading destination for illegal exports of restricted U.S. technology in the prosecutions brought in FY 2008, as well as those in FY 2007.

The illegal exports bound for Iran have involved such items as missile guidance systems, Improvised Explosive Device (IED) components, military aircraft parts, night vision systems and other materials. The illegal exports to China have involved rocket launch data, Space Shuttle technology, missile technology, naval warship data, Unmanned Aerial Vehicle or "drone" technology, thermal imaging systems, military night vision systems and other materials.

A significant portion of the cases in FY 2008 and in FY 2007 also involved illegal exports to Mexico. These prosecutions primarily involved illegal exports of firearms, including assault weapons and rifles, as well as large quantities of ammunition destined for Mexico. In addition, there were several cases during this period involving arms and other materials being routed to terrorist organizations in various nations.

New Counter-Proliferation Task Forces

The cornerstone of the initiative has been the ongoing formation of multi-agency Counter-Proliferation Task Forces in U.S. Attorney's offices around the country. Today, there are approximately 15 such task forces or working groups operating nationwide, some straddling more than one judicial district.

These entities have built on prior inter-agency efforts used in certain districts where agents from ICE, FBI, BIS, and Defense Department agencies pool data and jointly pursue cases. Under the leadership of U.S. Attorneys, these task forces foster coordination critical to the success of export control.

Enhanced Training and Coordination

Because export control cases involve complex statutory and regulatory schemes, sophisticated technology, international issues, agencies with different authorities, and, often classified information, training for prosecutors and agents has been a critical focus of the initiative.

Since January 2008 alone, the Justice Department's National Security Division has presented more than 30 legal training sessions and lectures around the country on export control. In addition, the Department has held two national export control training conferences and is scheduled to hold another in early 2009 in South Carolina. To date, more than 500 prosecutors and investigators have received training through these mechanisms.

The Department's National Security Division has also distributed a comprehensive tool kit of legal pleadings and related information on export control for field prosecutors and agents. On a daily basis, the National Export Control Coordinator provides legal advice and counsel for prosecutors and agents on these cases.

Another critical component of the initiative involves enhanced coordination within the export control community. The Justice Department, along with other agencies, has created the Technology Protection Enforcement Group (TPEG), an inter-agency Headquarters-level working group, to enhance export control coordination among law enforcement agencies and between law enforcement agencies and the Intelligence Community. In addition, the Department has created a working group of intelligence analysts to assist field prosecutors across the country in export cases and to ensure appropriate information sharing with the Intelligence Community.

The Department has also initiated monthly coordination meetings with the export licensing agencies, particularly the State Department's Directorate of Defense Trade Controls and the Commerce Department's BIS, to improve coordination and the flow of information to those agencies in accomplishing their missions. Furthermore, the Department regularly participates in and contributes to outreach efforts with foreign governments on export control matters, in conjunction with the State Department.

New Legislation

Over the past year, the Department has also been involved in a variety of legislative, regulatory, and policy proposals related to export control and embargos. During 2007, for instance, Congress passed and the President signed into law amendments to the International Emergency Economic Powers Act (IEEPA), which, among other things, added conspiracy and attempt provisions to the IEEPA as well as enhanced criminal fines and administrative fines for violations of this law, which is a critical export and embargo enforcement statute.

"We will not allow the United States' national security to be held hostage by rogue nations or sold to the highest bidder. This includes sensitive military information and technology, as well as weapons of mass destruction or the components needed to produce them. ICE is committed to working closely and cooperatively with our partners at every level of law enforcement to ensure this does not happen." Julie L. Myers, Assistant Secretary of Homeland Security for ICE said. "Time after time, our export enforcement investigations have helped prevent the illegal acquisition of these resources and helped maintain military, political and economic stability throughout the world."

"No one agency can accomplish the immense task of safeguarding U.S. national security assets and protecting the illegal export of restricted materials, including military and dual-use technologies," said Executive Assistant Director Arthur M. Cummings, II, of the FBI's National Security Branch. "The FBI is committed to enforcing export control laws and will continue to work closely with our partners in the law

enforcement and the intelligence communities to enhance export control awareness and training and to build on the success of our Counter-Proliferation Task Forces."

"We are continuing to sharpen our enforcement efforts to focus on those areas of greatest concern to us: proliferators, supporters of terrorism, and nations of illicit trans-shipment concern. When foreign companies take controlled U.S. technology and illegally transfer it - they also face serious repercussions. We remain committed to investigate, uncover, and stop these activities wherever they may occur," said Under Secretary of Commerce Mario Mancuso.

"Preventing the illegal export of critical technologies and restricted munitions is of extreme concern to the Department of Defense because of the real possibility that our Soldiers, Sailors, Airmen, and Marines may have to face this materiel in the hands of our adversaries and thereby lose the advantage that U.S. technology is supposed to provide them," said Charles W. Beardall, Department of Defense Deputy Inspector General for Investigations. "Protecting America's Warfighters through technology protection is a top priority for the Defense Criminal Investigative Service, the law enforcement arm of the DoD Inspector General, and a fundamental focus for our special agents."

"We applaud the Department of Justice's efforts," said John Rood, Acting Undersecretary of State for Arms Control and International Security. "We are pleased that the Department of State has been able to support this important initiative and proud of the tremendous success achieved so far in disrupting the flow of sensitive technology to our adversaries and protecting our national security and foreign policy interests."

Foreign Efforts to Obtain Controlled U.S. Technology

The technology at the heart of this initiative includes restricted U.S. military items, dual-use equipment, and other technical expertise or know-how, some of which have applications in Weapons of Mass Destruction. These materials are generally restricted and may not be exported without U.S. government approval. Foreign procurement networks intent on obtaining such materials from the U.S. rarely target complete weapons systems, but often focus on seemingly innocuous components to develop their own weapons systems.

According to recent reports by the Intelligence Community, private-sector businessmen, scientists, students, and academics from overseas are among the most active collectors of sensitive U.S. technology. Most did not initially come to the U.S. with that intent, nor were they directed to do so by foreign governments. Instead, after finding that they had access to technology in demand overseas, they engaged in illegal collection to satisfy a desire for profits, acclaim, or patriotism to their home nations.

At the same time, foreign government organizations remain aggressive in illegally acquiring sensitive U.S. technology. Some governments have established quasi-official organizations in the U.S. to facilitate contact with overseas scientists, engineers and businessmen. Foreign governments have been observed directly targeting U.S. firms; employing commercial firms in the U.S. and third countries to acquire U.S. technology; and recruiting students, professors, and scientists to engage in technology collection.

Fact Sheet

###

08-958

RELEASE

Department of Justice

FOR IMMEDIATE RELEASE
Tuesday, October 28, 2008
WWW.USDOJ.GOV

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

Fact Sheet: Major U.S. Export Enforcement Prosecutions During the Past Two Years

Below is a snapshot of some of the major export and embargo-related criminal prosecutions handled by the Justice Department over the past two years, beginning in October 2006. These cases resulted from investigations by the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE), the Federal Bureau of Investigation (FBI), the Department of Commerce's Bureau of Industry and Security (BIS), the Pentagon's Defense Criminal Investigative Service (DCIS), and other law enforcement agencies. This list of cases is not exhaustive and only represents select cases.

- ***Carbon-Fiber Material with Rocket & Spacecraft Applications to China*** – On Oct. 28, 2008, a grand jury in the District of Minnesota returned an indictment charging Jian Wei Deng, Kok Tong Lim, and Ping Cheng with conspiring to illegally export to the People's Republic of China (PRC) controlled carbon-fiber material with applications in aircraft, rockets, spacecraft, and uranium enrichment process. According to the indictment, the intended destination for some of the materials was the China Academy of Space Technology, which oversees research institutes working on spacecraft systems for the PRC government. Jian Wei Ding and Kok Tong Lim are residents of Singapore and affiliated with a Singaporean import/export company known as FirmSpace, Pte Ltd. Ping Cheng is a resident of New York and the sole shareholder of Prime Technology Corporation. This investigation was conducted by BIS and ICE.

- ***Violation of Trade Embargo with Iran*** – On Oct. 15, 2008, Seyed Mahmood Mousavi, a former interrogator for the Islamic Revolutionary Court in Iran, was sentenced in the Central District of California to 33 months in prison and a $12,500 fine for violating the trade embargo with Iran, false statements to the FBI, and filing a false tax return. Mousavi entered into consulting contracts to support a company in Iran in their efforts to bid for a mobile communication license and to establish a bank and leasing company in Iran. On April 24, 2008, Mousavi was convicted at trial of all counts of a June 8, 2007 indictment. The investigation was conducted by the FBI.

- ***Telecommunications Equipment to Iraq*** – On Oct. 2, 2008, Dawn Hanna was convicted by a jury in the Eastern District of Michigan on eight counts of an indictment charging her with illegally exporting telecommunications and other equipment with potential military applications to Iraq during the administration of Saddam Hussein and during the embargo on that country. Co-defendant Darrin Hanna was acquitted at trial. On July 19, 2007, both defendants were indicted on charges of conspiracy, violating the International Emergency Economic Powers Act, money laundering conspiracy, and false statements. From 2002 to 2003, the defendants allegedly received $9.5 million in proceeds to supply telecommunications and other equipment to Iraq in violation of the U.S. embargo that existed prior to the invasion by coalition forces in 2003. This investigation was conducted by ICE, the Internal Revenue Service (IRS) and the FBI.

- ***Military Accelerometers to China*** – On Sept. 26, 2008, Qing Li was sentenced in the Southern District of California to 12 months and one day in custody, followed by three years of supervised released, and ordered to pay $7,500 for conspiracy to smuggle military-grade accelerometers from the United States to the People's Republic of China (PRC). Li pleaded guilty on June 9, 2008 to violating Title 18, USC Section 554. She was indicted for the offense on Oct. 18, 2007. According to court papers, Li conspired with an individual in China to locate and procure as many as 30 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 *g*-forces of nuclear and chemical explosions. The investigation was conducted by ICE and the DCIS.

- ***Space Launch Technical Data and Services to China*** – On Sept. 24, 2008, Shu Quan-Sheng, a native of China, naturalized U.S. citizen and PhD physicist, was arrested in the Eastern District of Virginia on charges of illegally exporting space launch technical data and services to the People's Republic of China (PRC) and offering bribes to Chinese government officials. Shu was the President, Secretary and Treasurer of AMAC International, a high-tech company located in Newport News, Va., and with an office in Beijing, China. According to the complaint, beginning in or around January 2003, Shu provided technical assistance and foreign technology acquisition expertise to several PRC government entities involved in the design, development, engineering and manufacture of a space launch facility in the southern island province of Hainan, PRC. This facility will house liquid-propelled heavy payload launch vehicles designed to send space stations and satellites into orbit, as well as provide support for manned space flight and future lunar missions. Among those PRC government entities involved in the Hainan space launch facility the People's Liberation Army's General Armaments Department and the 101st Research Institute (101 Institute). Shu is accused of illegally exporting technical data related to the design and manufacture of a "Standard 100 M3 Liquid Hydrogen (LH) 2 Tank," and illegally providing assistance to foreign persons in the design, development, assembly, testing or modification of the "Standard 100 M3 LH2 Tank" and related components of fueling systems for a foreign launch facility. The complaint also alleges that Shu offered bribes to government officials with the PRC's 101 Institute to induce the award of a hydrogen liquefier project to a French company he represented. This investigation was conducted by the FBI, ICE, BIS and DCIS.

- ***Electronics & IED Components to Iran*** – On Sept. 18, 2008, a 13-count indictment was unsealed in the Southern District of Florida charging eight individuals and eight companies with conspiracy, violations of the International Emergency Economic Powers Act, the U.S. Iran embargo, and false statements in connection with their participation in conspiracies to illegally export electronics, Global Positioning Systems (GPS) systems, and other dual-use commodities to Iran. All the items had potential military applications, including in the construction of Improvised Explosive Devices (IEDs). Among other things, the indictment alleges the defendants illegally exported to Iran 345 GPS systems and 12,000 Microchip brand microcontrollers. These specific types of microcontrollers have been found in IEDs in Iraq. The businesses charged are: Mayrow General Trading, Atlinx Electronics, Micatic General Trading, Madjico Micro Electronics, and Al-Faris, all Dubai-based businesses; Neda Industrial Group, an Iran-based business; and Eco Biochem Sdn BHD and Vast Solution Sdn BHD, Malaysian businesses. The individuals charged are charged are: Ali Akbar Yahya and Farshid Gillardian, both Iranian nationals who are naturalized British citizens; F.N. Yaghmaei, Bahman Ghandi, Ahmad Rahzad, all Iranian nationals; Kaam Chee Mun, a resident of Malaysia; Djamshid Nezhad, a resident of Germany; and Majid Seif, an Iranian national residing in Malaysia. As part of the enforcement action, the Department of Commerce added 75 individuals and companies affiliated with this Iranian procurement network to its Entities list. This investigation was conducted by Commerce BIS, DCIS, ICE, and the Treasury Department's Office of Foreign Assets Control (OFAC.)

- ***Rifle Scopes to Russia*** – On Sept. 11, 2008, a grand jury in the Middle District of Pennsylvania indicted Boris Gavrilov, D&B Compas Ltd, and Kiflet Arm on charges of illegally exporting military-

grade and dual-use rifle scopes to Russia without the required U.S. government licenses. Gavrilov is believed to be a resident of Israel. D&B Compas is located in Israel, while Kiflet Arm is located in Humboldt, Texas. Extradition proceedings for Gavrilov have commenced. The investigation was conducted by ICE and BIS.

- ***Controlled Technology to Indian Missile & Space Facility*** – On Sept. 9, 2008, in the District of Columbia, a grand jury returned a five-count indictment against Siddabasappa Suresh, an Indian national, and Rajaram Engineering Corporation, an Indian corporation, on charges of illegally supplying the Government of India with controlled goods and technology without the required licenses. According to the indictment, from 2001 to 2003, Suresh and Rajaram caused the illegal export of more than 100 controlled goods with an approximate value of $136,000. The indictment specifically identified six shipments to Vikram Sarabhai Space Centre (VSSC), which was within the Department of Space of the Government of India and responsible for research, development, and production of India's space launch system. These activities encompassed both civilian spacecraft and ballistic missiles. All of these transactions involved complex electronic instruments used in high performance testing and monitoring essential in the research and development of launching systems, including missile delivery systems. The investigation was conducted by the Department of Commerce BIS.

- ***Fighter Jet Components to Iran*** -- On Sept. 5, 2008, George Frank Myles, Jr. pleaded guilty to conspiring to illegally export military aviation parts without obtaining the permission of the State Department, in violation of the Arms Export Control Act. Myles was indicted for this offense on Sept. 6, 2007 in the Southern District of New York, and the case was transferred to the Southern District of Florida pursuant to Rule 21. Sentencing is set for October 30, 2008. During the conspiracy, which spanned from April 2005 to March 2007, Myles supplied a number of military aviation parts, including F-14 parts, to an Iranian national, who allegedly picked up the parts in Dubai, United Arab Emirates and Bangkok, Thailand. This investigation was conducted by ICE.

- ***Ammunition to Mexico*** – On Sept 5, 2008, Noe Guadalupe Calvillo, Juan Luis Hernandez-Ramos, Guadalupe Ramiro Munoz-Mendez and Rogelio Garcia were sentenced to 46 months in prison, 37 months in prison, 30 months in prison, and 39 months in prison, respectively, after pleading guilty to illegally exporting thousands of rounds of ammunition to Mexico. Calvillo pleaded guilty to illegally exporting 51,400 rounds of ammunition, while Garcia, Hernandez-Ramos and Munoz-Mendez pleaded guilty to exporting 30,900 rounds of ammunition. The defendants were arrested and charged in Oct. 2007. This investigation was conducted by ICE.

- ***Military Technical Data on Unmanned Aerial Vehicles to China*** – On Sept. 3, 2008, J. Reece Roth, a former Professor Emeritus at the University of Tennessee, was convicted in the Eastern District of Tennessee of 15 counts of violating the Arms Export Control Act, one count of conspiracy, and one count of wire fraud. Roth had illegally exported military technical information relating to plasma technology designed to be deployed on the wings of Unmanned Aerial Vehicles (UAVs) or "drones" operating as a weapons or surveillance systems. The illegal exports involved technical data and information related to a U.S. Air Force research and development contract that Roth provided to foreign nationals from China and Iran. In addition, Roth carried multiple documents containing controlled military data with him on a trip to China and caused other controlled military data to be e-mailed to an individual in China. On Aug. 20, 2008, Atmospheric Glow Technologies, Inc (AGT), a privately-held plasma technology company in Tennessee, also pleaded guilty to charges of illegally exporting U.S. military data about drones to a citizen of China in violation of the Arms Export Control Act. Roth and AGT were first charged on May 20, 2008 in an 18-count indictment. In a related case, on April 15, 2008, Daniel Max Sherman, a physicist who formerly worked at AGT, pleaded guilty to an information charging him with conspiracy to violate the Arms Export Control Act in connection with this investigation. The investigation was conducted by the FBI, ICE, U.S. Air Force Office of Special Investigations, DCIS and BIS.

- ***Military Aircraft Components to China and Iran*** -- On Aug. 28, 2008, Desmond Dinesh Frank, a citizen and resident of Malaysia, was sentenced to 23 months in prison after pleading guilty on May 16, 2008, to several felonies in the District of Massachusetts in connection with a plot to illegally export military items to China and Iran. A six-count indictment returned on Nov. 15, 2007 charged Frank, the operator of Asian Sky Support, Sdn., Bhd., in Malaysia, with conspiring to illegally export items to Iran, conspiring to illegally export C-130 military aircraft training equipment to China, illegally exporting defense articles, smuggling, and two counts of money laundering. Frank was arrested in Hawaii on Oct. 8, 2007 by ICE agents. Frank conspired with others to illegally export and cause the re-export of goods, technology and services to Iran without first obtaining the required authorization from the Treasury Department. He also conspired with others to illegally export ten indicators, servo driven tachometers -- which are military training components used in C-130 military flight simulators -- from the United States to Malaysia and ultimately, to Hong Kong, China, without the required license from the State Department. This investigation was conducted by ICE, BIS, and DCIS.

- ***Forklift Parts to Iran*** – On Aug. 26, 2008, Robert E. Quinn pleaded guilty in the District of Colombia to a criminal information filed on July 9, 2008 alleging that he knowingly made false statements in connection with the illegal export of forklift parts to Iran. On Aug. 4, 2006, David Tatum was sentenced to one year probation and a $5,000 fine, in connection with the illegal export of forklift parts to Iran by Clark Material Handling Corporation via Sharp Line Trading in Dubai, United Arab Emirates. On Jan. 19, 2006, Khalid Mamood, doing business as Sharp Line Trading, was sentenced to 17 months in prison. The case was investigated by ICE and BIS.

- ***Thermal Imaging Cameras to China*** -- On Aug. 25, 2008, in the Central District of California, an individual pleaded guilty to one count of exporting national security controlled items without obtaining the necessary license in violation of the International Emergency Economic Powers Act and the Export Administration Regulations. The defendant served as the President of an Ohio company involved in the development of high tech commodities, including infrared thermal imaging devices. In February 2007, the defendant illegally exported infrared thermal imaging cameras to Zhi Yong Guo, the managing director of Beijing Shenzhoukaiye System Engineering Technology Research Center in Beijing, China. The defendant is the second person to plead guilty in this case, which involves two additional defendants. On July 16, 2008, Tah Wei Chao, of Beijing, China, pleaded guilty to one count of conspiracy and two counts of illegally exporting or attempting to restricted items. Zhi Yong Guo, a Chinese national, is scheduled to stand trial in October 2008, on one count of conspiracy and one count of illegally exporting or attempting to restricted items. Both Chao and Guo were arrested at the Los Angeles International Airport in April 2008 after authorities recovered 10 cameras hidden in their suitcases. They were charged on April 7, 2008. The investigation was conducted by BIS, ICE, FBI, and other federal agencies.

- ***Military Laser Aiming Devices & Fighter Pilot Cueing Systems to Taiwan*** – On Aug. 18, 2008, Yen Ching Peng was arraigned in Southern District of New York on Arms Export Control Act violations, as well as money laundering and smuggling violations after being extradited from Hong Kong. Among other things, Peng allegedly attempted to illegally export to Taiwan infrared laser aiming devices, thermal weapons sights, and a Joint Helmet Mounted Cueing System. On occasion, Peng requested that military items be delivered to his associate, Peter Liu, in New York for delivery in Taiwan. On Dec. 11, 2007, Peng was arrested in Hong Kong, while Liu was arrested in New York. Liu later pleaded guilty and was sentenced to 30 months in prison on Aug. 7, 2008. The investigation was conducted by ICE and DCIS.

- ***Missile Technology to Indian Government Entities*** -- On Aug. 11, 2008, in the District of Columbia, Mythili Gopal was sentenced to four years' probation and fined $5,000 after pleading guilty on Oct. 30, 2007 to one count of conspiracy to violate the International Emergency Economic Powers Act and the Arms Export Control Act. Gopal cooperated with the government against her co-conspirator,

Parthasarathy Sudarshan, who on June 16, 2008, was sentenced to 35 months in prison. Sudarshan, the owner of an international electronics company called Cirrus Electronics, pleaded guilty in March 2008 to conspiring to illegally export 500 controlled microprocessors and other electronic components to government entities in India that participate in the development of ballistic missiles, space launch vehicles, and combat fighter jets. Among the recipients of the U.S. technology were the Vikram Sarabhai Space Centre and Bharat Dynamics, Ltd., two Indian entities involved in ballistic missile production, as well as the Aeronautical Development Establishment, which is developing India's Tejas fighter jet. Sudarshan was one of four defendants indicted in the case on March 8, 2007. Sudarshan and Gopal were arrested in South Carolina on March 23, 2007. The other two defendants, Akn Prasad and Sampath Sundar remain at large. Court documents in the case indicate Sudarshan was working with an Indian government official located in Washington, D.C. as part of the conspiracy. The investigation was conducted by the FBI, BIS, and ICE.

- ***Equipment to Iran*** – On Aug. 11, 2008, Nicholas D. Groos entered a guilty plea in the Northern District of Illinois to three counts of violating the International Emergency Economic Powers Act and one count of making false statements in connection with a scheme to transship U.S.-origin firefighting equipment to Iran using his position as director of a Viking Corporation subsidiary in Luxemburg. Groos was indicted on May 3, 2007. The case was investigated by ICE and BIS.

- ***Engineering Software to Iran*** – On Aug. 7, 2008, James Angehr and John Fowler, the owners of Engineering Dynamics, Inc. were sentenced to five years probation, fined $250,000 and ordered to forfeit $218, 583. On April 24, 2008, both pleaded guilty to a one-count information charging them with conspiring to violate the International Emergency Economic Powers Act in connection with a plot to export controlled engineering software to Iran. Engineering Dynamics, Inc, was a Louisiana company that produced software to design offshore oil and gas structures. As part of the case, on May 22, 2008, in the Eastern District of Louisiana, Nelson S. Galgoul, a resident of Brazil and the director of Suporte, a Brazilian engineering company, was sentenced to 13 months in prison for violating the International Emergency Economic Powers Act. Galgoul pleaded guilty on Aug. 2, 2007, to exporting and attempting to export controlled engineering software to Iran without the required U.S. authorization. Galgoul was charged in May 2007. He acted as an agent for Engineering Dynamics, Inc. in the marketing and support of this software and trained users of the software in Iran. As part of the same case. The investigation was conducted by ICE, BIS and FBI.

- ***Night Vision Goggles to Pakistan, Italy, South Korea*** – On July 31, 2008, Rigel Optics, Inc., pleaded guilty in the Southern District of Iowa to one count of violating the Arms Export Control Act in connection with an illegal export of night vision goggles, while its President, Donald Wayne Hatch, pleaded guilty to one count of false statements in connection with the case. The defendants were indicted on June 24, 2008 for illegally exporting military night vision systems to Pakistan, Italy, and South Korea. The investigation was conducted by ICE and BIS

- ***Telecommunications Systems to Iran*** – On July 28, 2008, Allied Telesis Labs, Inc. was sentenced in the Eastern District of North Carolina to a $500,000 criminal fine and was placed on probation for two years. The company pleaded guilty on March 18, 2008, to conspiracy to violate the International Emergency Economic Powers Act as part of a scheme to land and execute a $95 million contract with the Iranian Information Technology Company to rebuild the telecommunications systems of 20 Iranian cities. The company was first charged via criminal information on Jan. 23, 2008. The investigation was conducted by BIS.

- ***Infrared Assault Rifle Scopes to Indonesia*** -- On July 28, 2008, in the Western District of Wisconsin, Doli Syarief Pulungan was sentenced to 48 months in prison followed by three years supervised release. On May 6, 2008, Pulungan, a citizen of Indonesia, was convicted of conspiracy to violate the Arms Export Control Act in connection with a plot to illegally export 100 Leupold Mark 4

CQ/T Riflescopes to Indonesia. Pulungan was first charged on Oct. 1, 2007. The tactical riflescopes have infrared capability and are designed to attach to M-16 and AR-15 assault rifles. The investigation was conducted by the FBI.

- ***Night Vision Firearm Sights to Japan*** – On July 28, 2008, Tomoaki Ilshiba, a U.S. Army Captain, pleaded guilty in the Western District of Washington to conspiracy to smuggle goods from the United States. In his plea agreement, Iishiba admitted that he illegally shipped firearms parts including holographic night vision firearms sights to contacts in Japan. In October and December 2006, Iishiba shipped sixty holographic sights to a contact in Japan and purposely mislabeled the customs form for the shipment because he knew he needed a license to ship the firearms parts to Japan. Iishiba was charged on July 16, 2008. This investigation was conducted by ICE, DCIS, and the Army Criminal Investigation Command.

- ***Chemical Purchasing Software to Iran*** – On July 25, 2008, Ali Amirnazmi, the owner of Trantech Consultants, Inc., in Pennsylvania, was indicted in the Eastern District of Pennsylvania, for acting as an unregistered agent of the Iranian government, violating U.S. sanctions against Iran, and for lying to federal agents. For more than a decade, Amirnazmi allegedly sold software designed to help buyers around the globe locate the best prices for various chemicals to several Iranian companies that were owned in part or in whole by the Iranian government. This investigation was conducted by the FBI and IRS.

- ***Combat Gun sights to Sweden and Canada*** – On July 24, 2008, Euro Optics Inc., was sentenced in the Middle District of Pennsylvania to a $10,000 corporate fine, $800 special assessment, and five years of corporate probation after pleading guilty on March 17, 2008 to illegally exporting advanced combat gun sights to Sweden and Canada without the required licenses. Euro Optics was charged via criminal information on Oct. 5, 2007. This investigation was conducted by ICE and Department of Commerce BIS.

- ***Cryogenic Pumps to Iran*** – On July 17, 2008, Cryostar SAS, formerly known as Cryostar France, a corporation headquartered in France, was sentenced in the District of Columbia to a criminal fine of $500,000 and corporate probation of two years. On April 11, 2008, the company pleaded guilty to conspiracy, illegal export, and attempted illegal export of cryogenic submersible pumps to Iran without a license. Cryostar specialized in the design and manufacturing of cryogenic equipment, such as pumps, that are used to transport and process natural gases at extremely cold temperatures. The company was charged on March 24, 2008. The investigation was conducted by BIS.

- ***Military Aircraft Components to UAE, Thailand*** – On July 17, 2008, in the Central District of California, Air Shunt Instruments, Inc., was sentenced to pay a criminal fine of $250,000 and a special assessment of $400 for making false statements on Shipper's Export Declaration in claiming that a military gyroscope being sent overseas in 2003 did not require an export license, when in fact the item required such a license. Air Shunt, a Chatsworth, California company that buys and sells aircraft and aerospace components, was charged via criminal information and pleaded guilty on July 15, 2008. John Nakkashian, a Vice President for International Sales at Air Shunt, was responsible for obtaining the required licenses for such exports. During the investigation, Nakkashian fled the country and remains a fugitive today. On May 20, 2008, Nakkashian was indicted on four counts of violating the Arms Export Control Act. The indictment alleges he illegally exported components for the J85 engine, used on the F-5 fighter jet, and other military items to Dubai, United Arab Emirates, without first obtaining the required export license from the State Department. The indictment also alleges that he illegally exported a military gyroscope to Thailand. The investigation was conducted by DCIS and ICE.

- ***Cuba*** – On July 15, 2008, Platte River Associates, a Colorado company, was charged in U.S. District

Court in Denver by Information for trading with the enemy. The president of Platte River Associates, Jay E. Leonard, was charged in separate Information on July 15, 2008, for unauthorized access of a protected computer. According to the Platte River Associates Information, on or about October 2000, the corporation allegedly provided specialized technical computer software and computer training, which was then used to create a model for the potential exploration and development of oil and gas within the territorial waters of Cuba, without first having obtained a license. This case was investigated by ICE. In the second case, Leonard allegedly used a wireless network connection at Houston International Airport to access a password protected computer website server located in Georgia, belonging to Zetaware Inc., a Texas Corporation. The Information charges that the unauthorized information obtained by the defendant was done by means of interstate commerce. This case was investigated by the FBI .

- ***Surface-to-Air Missiles, Night Vision Devices, Firearms to Foreign Terrorists*** – On July 10, 2008, Erik Wotulo, a retired Indonesian Marine Corps general, was sentenced in the District of Maryland to 30 months in prison for conspiracy to provide material support to terrorists (the Liberation Tigers of Tamil Eelam or Tamil Tigers), and money laundering. According to the plea agreement, beginning in April 2006, Wotulo conspired with Haji Subandi, Haniffa Bin Osman and Thirunavukarasu Varatharasa to export state-of-the-art firearms, machine guns and ammunition, surface to air missiles, night vision goggles and other military weapons to the Tamil Tigers operating in Sri Lanka, to be used to fight against Sri Lankan government forces. The conspirators contacted an undercover business located in Maryland about the sale of military weapons. In September 2006, the defendants arrived in Guam, where they met with undercover officers to inspect and take possession of the weapons, and were eventually arrested. On Jan. 3, 2008, Varatharasa was sentenced to 57 months in prison. Subandi was sentenced to 37 months in prison on Dec. 14, 2007, while Osman is scheduled to be sentenced in August 2008. Two additional defendants, Rinehard Rusli and Helmi Soedirdja, pleaded guilty to export and money laundering violations on Jan. 30, 2007, as part of a related plot to provide military night vision devices to the Indonesian military. The investigation was conducted by ICE, the FBI, and DCIS.

- ***Military Night Vision Systems to Lebanon*** – On July 9, 2008, Riad Skaff, a naturalized U.S. citizen from Lebanon and former ground services coordinator at O'Hare International Airport, was sentenced in the Northern District of Illinois to two years in prison for using his position at the airport to help smuggle $396,000 in cash and illegally export weapons scopes, military night vision goggles, and a cellular phone "jammer" to Lebanon. The case resulted from an undercover operation in which agents posed as individuals interested in smuggling money and military items to Lebanon utilizing contacts at O'Hare airport to bypass security. On Aug. 17, 2007, Skaff pleaded guilty to all nine counts of an indictment charging him with bulk cash smuggling; entering an aircraft and airport area in violation of applicable security requirements with the intent to commit a felony; exporting and attempted export of defense articles without first obtaining a required export license; and attempted international export of merchandise, articles, and objects contrary to U.S. law. Skaff was first arrested on Jan. 28, 2007. The investigation was conducted by ICE and DCIS.

- ***Stolen Software to Iran*** – On June 25, 2008, Mohammad Reza Alavi pleaded guilty to transporting stolen property in interstate commerce, in connection with his theft of software belonging to the Palo Verde Nuclear Generating station in Arizona that was valued at $400,000. On May 28, 2008 a jury also convicted Alavi of unauthorized access to a protected computer, but deadlocked on charges that he illegally exported the software. Alavi is a former employee of the Palo Verde nuclear plant, the largest in the United States, and served as a software engineer in the Simulator Support Group which maintained a simulator system to train control room employees on the operation of nuclear reactors. The simulator system utilizes software called "3KeyMaster" to replicate current reactor status at Palo Verde allowing an operator to artificially create various incidents to train employees on safety and protocol procedures. The government presented evidence at trial that, after Alavi gave Palo Verde notice of his intent to terminate employment, he installed the "3KeyMaster" software on his personal laptop without permission of Palo Verde. Alavi then took the software to Iran. Alavi's

conduct was uncovered when he accessed the software vendor's website from Iran and obtained a code which allowed the software to be unlocked and activated. Alavi was indicted on April 12, 2007, following his arrest that month upon returning to the U.S. Following his arrest, Alavi admitted he took the software to help him obtain future employment in the nuclear field. The FBI conducted the investigation.

- ***Fighter Jet and Military Helicopter Components to Iran*** – On July 3, 2008, Hassan Saied Keshari, Traian Bujduveanu, Kesh Air International, and Orion Aviation Corp, were indicted in the Southern District of Florida for conspiring to violate the International Emergency Economic Powers Act, the U.S. Iran Embargo, and the Arms Export Control Act for their participation in a conspiracy to export U.S.-made military aircraft parts to Iran. On June 20, 2008, agents arrested Keshari at Miami International Airport as he walked off a flight from Atlanta. Bujduveanu was arrested at his Plantation, Florida, home on June 21, 2008. Keshari owns and operates Kesh Air International, a business located in Novato, California. Bujduveanu owns and operates Orion Aviation Corp., located in Plantation, Florida. Since August 2006, Keshari and Bujduveanu have allegedly procured U.S.-made military aircraft parts for buyers in Iran and have illegally shipped the parts to a company in Dubai, UAE, for shipment to buyers in Iran. Keshari allegedly received the orders for specific parts by e-mail from buyers in Iran. Keshari then requested quotes, usually by e-mail, from Bujduveanu and made arrangements with Bujduveanu for the sale and shipment of the parts to a company in Dubai. From Dubai, the parts were then shipped on to Iran. Keshari and Bujduveanu are alleged to have obtained and illegally shipped to buyers in Iran parts for the CH-53 military helicopter, the F-14 Tomcat fighter jet, and the AH-1 attack helicopter. Keshari is also alleged to have requested quotes for other parts for other military aircraft, including F-4 Phantom aircraft. This investigation was conducted by BIS, ICE, and DCIS.

- ***Illegal Export of F-5 and F-14 Fighter Jet Components*** – On June 19, 2008, in the Southern District of New York, Jilani Humayun, a Pakistani citizen and resident of Long Island, New York, pleaded guilty to conspiracy to illegally export arms and to commit money laundering. He faces a maximum sentence of 30 years and a $1 million fine. Humayun was arrested on July 19, 2007, and charged by information on December 19, 2007, with Conspiracy to Violate the Arms Export Control Act and Smuggle Goods from the United States, and Conspiracy to Violate the International Emergency Economic Powers Act. According to his plea, Humayun illegally exported parts for F-5 and F-14 military fighter jets to Malaysia which prosecutors said may have eventually ended up in Iran. In the process of exporting these parts, he created airway bills that misrepresented the contents and value of his shipments. Such exports are of particular concern because F-14 components are widely sought by Iran, which is currently the only nation in the world that still flies the F-14 fighter jet. Humayun formed his own company, Vash International, Inc., in 2004, then, on eleven separate occasions between January 2004 and May 2006, exported to Malaysia F-5 and F-14 parts, as well as Chinook Helicopter parts. This investigation was conducted by ICE, BIS, FBI and DCIS.

- ***Firearms to Canada*** – On June 19, 2008, Ugur Yildiz was arrested and charged in a criminal complaint in the Northern District of Illinois with illegally exporting some 220 firearms from Chicago to Canada in 2006. The investigation was conducted by ICE and the ATF.

- ***U.S. Military Source Code and Trade Secrets to China*** – On June 18, 2008, Xiaodong Sheldon Meng was sentenced in the Northern District of California to 24 months in prison, three-years of supervised release, and a $10,000 fine for committing economic espionage and violating the Arms Export Control Act. Meng pleaded guilty in August 2007 to violating the Economic Espionage Act by misappropriating a trade secret used to simulate motion for military training and other purposes, with the intent to benefit China's Navy Research Center in Beijing. He also pleaded guilty to violating the Arms Export Control Act for illegally exporting military source code involving a program used for training military fighter pilots. Meng was the first defendant in the country to be convicted of exporting military source code pursuant to the Arms Export Control Act. He was also the first defendant to be

sentenced under the Economic Espionage Act. Meng was charged in a superseding indictment on Dec. 13, 2006. The investigation was conducted by FBI and ICE.

- ***Valves to Iran*** – On June 9, 2008, CVC Services was sentenced in the Central District of California to a fine of $51,000 and five years probation for illegal transactions with Iran. In March 2008, the company pleaded guilty to selling to Iran valves that turn gas and oil pipelines on and off without a license. The company was charged on Jan. 31, 2008. The National Iranian Oil Company had sought the valves. This investigation was conducted by BIS.

- ***Controlled Amplifiers to China*** – On June 6, 2008, WaveLab, Inc. of Reston, Virginia, was sentenced in the Eastern District of Virginia to one year of supervised probation and a $15,000 fine, together with $85,000 in forfeiture previously ordered, for the unlawful export 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. WaveLab pleaded guilty on March 7, 2008 to a criminal information filed the same day. The investigation was conducted by BIS and ICE.

- ***Firearms Components to Sudan*** – On June 6, 2008, Khalid Abdelgadir Ahmed was sentenced in the Eastern District of Virginia to five months in prison after pleading guilty on March 13, 2008, to unlawfully attempting to export assault rifle components to the Sudan. Another defendant, Entisar Hagosman, was sentenced to time served and two years supervised probation on June 6, 2008 after pleading guilty on Mar. 13, 2008 to making false statements relating to her activity. Both defendants were charged in a complaint on Jan. 30, 2008. The investigation was conducted by ICE and BIS.

- ***Arms Exports to Russia*** – On June 6, 2008, the United States Attorney for the Middle District of Pennsylvania announced that a superseding indictment was returned against Russian nationals, Sergey Korznikov of Moscow, Mark Komoroski of Nanticoke, Pa, and two companies, D&R Sports Center and Tactica Limited. The indictment charged them with conspiring to smuggle military equipment, including rifle scopes, magazines for firearms, face shields, and other military equipment from the United States to Russian to be resold to unknown persons. The case was investigated by ICE, IRS, ATF, U.S. Postal Service, Department of Commerce and DCIS.

- ***Amplifiers / Missile Target Acquisition Technology to China*** – On June 5, 2008, a grand jury in the Southern District of Florida returned an indictment charging Joseph Piquet, AlphaTronX, Inc, Thompson Tam, and Ontime Electronics Technology Limited with violations of the Arms Export Control Act and the International Emergency Economic Powers Act in connection with a conspiracy to illegally export to China military amplifiers used in early warning radar and missile target acquisition systems. The defendants were also charged will illegally exporting controlled dual-use amplifiers that have military applications. Piquet is the owner and President of AlphaTronX, a company in Port St. Lucie, Florida, that produces electronic components. Tam is a director of Ontime Electronics, an electronics company in China. This investigation was conducted by BIS and ICE.

- ***Theft of Military Trade Secrets to Sell to Foreign Governments*** -- On May 16, 2008, Allen W. Cotten of El Dorado Hills, California, was sentenced in the Eastern District of California to two years in prison for theft of trade secrets. Cotten pleaded guilty on Feb. 29, 2008, admitting that while employed at Genesis Microwave Inc., he stole items including plans, designs and parts for the manufacture and testing of detector logarithmic video amplifiers (DLVA) and successive detection logarithmic video amplifiers (SDLVA), which are components used in microwave technologies. These technologies have military applications that include enhancing navigational and guidance capabilities; radar

jamming; electronic countermeasures; and location of enemy signals. Cotten sold and offered for sale these items to foreign governments and foreign military contractors. The total amount of actual or intended sales to these companies was $250,000. Cotten was charged by criminal information on Jan. 30, 2008. The investigation was conducted by the FBI and BIS.

- ***Controlled Computers to Iran*** – On May 15, 2008, Afshin Rezaei was sentenced in the Northern District of Georgia to six months' imprisonment and agreed to forfeit $50,000. Rezaei pleaded guilty on April 24, 2008 to one count of violating the International Emergency Economic Powers Act for the unlicensed export of computers to Iran via the United Arab Emirates. The computers were controlled for anti-terrorism reasons. Rezaei was indicted on Nov. 14, 2007. The investigation was conducted by BIS and ICE.

- ***Controlled Radiographic Equipment to Iran*** – On May 14, 2008, Bahram "Ben" Maghazehe pleaded guilty in the Southern District of New York to one count of false statements in connection with the illegal shipment of radiographic equipment to Iran. On August 14, 2007, Maghazehe and his associate Jeff Weiss were arrested pursuant to this shipment. The investigation was conducted by BIS.

- ***Ammunition to Jamaica, Defense Training to UAE*** -- On May 12, 2008, Lance Brooks was charged in the Southern District of Florida with being an unlicensed broker of defense articles in connection with his efforts to broker the sale of 270,000 rounds of soft point ammunition to the Jamaica Constabulatory Force without the required license from the State Department. The case marked the second time Brooks had been charged with arms export violations. On Dec. 20, 2007, Brooks pleaded guilty to charges brought in Oct. 2007 that he exported defense training services on grenade launchers to the United Arab Emirates without a license. He was on bond pending sentencing in that case when the new charges against him were filed. The investigation was conducted by the FBI.

- ***Test Tube and Microplate Coating Systems to Iran*** – On May 1, 2008, Patrick Gaillard, the owner of Oyster Bay Pump Works, Inc., was sentenced in the Eastern District of New York after pleading guilty to conspiracy to violate the International Emergency Economic Powers Act in connection with the planned export of restricted test tube and microplate coating systems to Iran through a trading company in the United Arab Emirates. The coating systems for microplates and test tubes produced by Oyster Bay are controlled for export and can be used in a wide variety of research and laboratory applications. On July 17, 2007, James Gribbon pleaded guilty to conspiracy to violate the Emergency Economic Powers Act in connection with the case. The investigation was conducted by BIS.

- ***Controlled Computer Equipment to Iran*** – On April 28, 2008, Mohammad Mayssami was sentenced in the Northern District of California to two years probation, a $10,000 fine and 160 hours of community service for his role in financing illegal exports to Iran. On Dec. 17, 2007, Mayssami pleaded guilty to failing to report a suspicious transaction for his part in financing export transactions by Super Micro Computer, Inc. He was originally charged by information on Dec. 3, 2007. Super Micro pleaded guilty on Sept. 18, 2006 to illegally exporting motherboards controlled for national security reasons to Iran and was sentenced to pay a criminal fine of $150,000., and agreed to pay an administrative fine of $125,400 to settle charges for related transactions. Super Micro was first charged on Sept. 1, 2006. The case was conducted by BIS.

- ***Military Night Vision Systems to Iran*** – On April 10, 2008, a British court ruled that Nosratollah Tajik should be extradited to the United States in connection with charges that he conspired to illegally export night vision weapons sights and military night vision goggles from the United States to Iran. Tajik plans to appeal the British High Court decision to the European Court of Human Rights. On Oct. 26, 2006, Tajik was arrested at his residence in County Durham in England by British law

enforcement authorities, pursuant to U.S. charges filed in the Northern District of Illinois on Aug. 30, 2006. From December 1999 to October 2003, Tajik served as the Iranian Ambassador to Jordan. Tajik also held an honorary fellowship at England's University of Durham's Institute for Middle East and Islamic Studies. According to the August 2006 U.S. complaint, Tajik and a co-conspirator, Esmaiil Gharekhani, conspired to export to a variety of prohibited items from the United States to Iran via the United Kingdom, including night vision weapon sights and night vision goggles. The co-conspirator sent purchase orders to ICE agents for several controlled articles and asked that the goods be shipped from the U.S. to the United Arab Emirates for transshipment to Iran. During meetings in the United Kingdom, Tajik also allegedly asked agents about procuring a Swiss-manufactured 35mm naval gun capable of intercepting guided missiles. This investigation was conducted by ICE.

- ***Russian Attack Helicopters to Zimbabwe*** – On April 8, 2008, Peter Spitz, a resident of Hallandale, Fla., and the owner of Russian Aircraft Services LLC, was arrested in Miami pursuant to a criminal complaint alleging that he conspired to sell seven MI-24 Russian attack helicopters and three MI-8T Russian military transport helicopters to undercover law enforcement officials who represented that the helicopters would be going to a Cabinet member of the government of Zimbabwe. Spitz was charged in the Southern District of Florida with illegal arms brokering activities. The investigation was conducted by ICE and DCIS.

- ***Trade Secrets to Chi* na** – 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. On April 21, 2008, Chi Mak's brother, Tai Mak, was sentenced to 10 years imprisonment pursuant to a June 4, 2007, plea agreement in which he pleaded guilty to one count of conspiracy to export defense articles. On Oct. 2, 2008, Chi Mak's wife, Rebecca Chiu, was sentenced to 3 years in prison for her role in the plot. The investigation was conducted by FBI, NCIS, and ICE.

- ***Specialty Alloy Pipes to Iran*** – On March 14, 2008, Proclad International Pipelines, Ltd, a British corporation headquartered in Scotland, was sentenced in the District of Columbia to a criminal fine of $100,000 and corporate probation of five years for attempting to export from the United States to Iran via the United Kingdom and United Arab Emirates specialty alloy pipes without an export license from the U.S. government. Proclad pleaded guilty to one count of attempted export without an export license on Nov. 30, 2007 after being charged via information on Oct. 16, 2007. The investigation was conducted by ICE and BIS.

- ***Nuclear Testing Equipment to India*** – On March 12, 2008, MTS Systems Corp, of Eden Prairie, Minnesota, pleaded guilty in the District of Minnesota to two misdemeanor counts and was sentenced to two years probation and a $400,000 fine for submitting false export license applications to the Department of Commerce in connection with the proposed shipment of seismic testing equipment with nuclear applications to an entity in India. MTS knew the end-user in India would likely use the seismic testing equipment for nuclear purposes, but, in its export applications to the Department of Commerce, MTS falsely certified that the equipment would be used only for non-nuclear purposes. Commerce denied the export license. The company was charged on March 11, 2008. The investigation was conducted by BIS and ICE.

- ***100,000 Uzi Submachine Guns to Iran*** – On March 10, 2008, Seyed Maghloubi was sentenced to three years and five months in prison in the Central District of California to attempting to illegally export goods to Iran. As part of his Aug. 27, 2007, plea agreement, Maghloubi admitted that he had plotted to illegally export as many as 100,000 Uzi submachine guns as well as night vision goggles to officials in Iran's government. According to the facts of the plea agreement, the defendant sought to have the weapons shipped from the U.S. to Dubai and later transported over the border to Iran. Maghloubi was first charged on June 1, 2007. The investigation was conducted by the FBI and the Los Angeles Police Department.

- ***International Arms Dealer Charged with Conspiracy to Provide Weapons to Terrorists*** : On March 6, 2008, a criminal complaint was unsealed in U.S. District Court for the Southern District of New York charging Viktor Bout, an international arms dealer, and his associate Andrew Smulian with conspiring to provide millions of dollars of weapons, including surface-to-air missiles and armor piercing rocket launchers, to the Fuerzas Armadas Revolucionarias de Colombia (FARC), a designated foreign terrorist organization based in Colombia. Bout was arrested on March 5, 2008 by Thai authorities in Bangkok, Thailand. According to the complaint, between November 2007 and February 2008, Bout and Smulian agreed to sell large quantities of weapons to two confidential sources working with the Drug Enforcement Administration (DEA) who held themselves out as FARC representatives acquiring these weapons for the FARC to use in Colombia. During one series of consensually recorded meetings in Romania, Smulian allegedly advised the confidential sources that Bout had 100 Surface-to-Air missiles available immediately; that Bout could also arrange to have a flight crew airdrop the weapons into Colombia using combat parachutes; and that Bout and Smulian would charge $5 million to transport the weapons. Bout engaged in multiple recorded phone calls with one of the DEA cooperating sources. The United States plans to pursue the extradition of Bout from Thailand. Smulian has already made his initial court appearance in the Southern District of New York. This investigation was conducted by the DEA.

- ***Controlled Computers to Syria*** – On Feb. 14, 2008, Mazen Ghashim was sentenced in the Southern District of Texas to three years probation for violating the International Emergency Economic Powers Act and attempted export without a license. He was also ordered to forfeit computers and related equipment valued at $32,000. The violations occurred in February 2003 when Ghashim and his company KZ Results exported computers and related equipment to Syria without the required licenses. Ghashim was charged on Aug. 14, 2006, and pleaded guilty on Nov. 1, 2006. This investigation was conducted by BIS.

- ***Theft of Trade Secrets on U.S. Space Shuttle for China*** – On Feb. 11, 2008, Dongfan "Greg" Chung, a former Boeing engineer, was 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, 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 NASA.

- ***Two Sentenced in Iranian Embargo Case*** -- On Feb. 8, 2008, in the District of Columbia, Mojtada Maleki-Gomi was sentenced to 18-months and a $200,000 fine for violating the U.S. embargo against Iran for conspiring to sell textile machinery to Iran. Maleki-Gomi's son, Babak Maleki, was sentenced on the same day to probation for making false statements. On Sept. 29, 2006, Maleki-Gomi, his son, and a third defendant, Shahram Setudeh Nejad, were indicted for conspiracy to violate the International Emergency Economic Powers Act and the Iranian Transactions Regulations, and for violation of the United States Iranian Embargo. On November 19, 2007, Maleki-Gomi pled guilty to the conspiracy charge and his son Babar Maleki pled guilty to a superseding information charging him with making false statements.

- ***Military & Commercial Aircraft Components to Iran*** – On Feb. 1, 2008, Laura Wang-Woodford, the director of a Singapore-based aviation company, was arraigned in the Eastern District of New York in connection with charges that she illegally exported controlled U.S. commercial and military aircraft components to Iran. She pleaded not guilty and was ordered detained. Wang-Woodford is a U.S. citizen who served as the director of Monarch Aviation Pte, Ltd., a company in Singapore that has imported and exported aircraft components for more than 16 years. She and her husband, Brian D. Woodford, were charged in a 20-count indictment with Arms Export Control Act and International Emergency Economic Powers Act violations in the Eastern District of New York. According to the indictment, Wang-Woodford exported controlled U.S. aircraft parts from the United States to her company in Singapore and then re-exported these commodities to a company in Tehran, Iran without obtaining the required U.S. Government licenses. A superseding indictment against the couple was returned on May 27, 2008. At the time of her Dec. 23, 2007 arrest in San Francisco, Wang-Woodford was carrying catalogues from the China National Precision Machinery Import and Export Company (CPMIEC), which contained advertisements for surface-to-air missiles and rocket launchers. CPMIEC has been sanctioned by the Treasury Department as a specially designated Weapons of Mass Destruction proliferator. The investigation was conducted by BIS and ICE.

- ***Military Night Vision Systems Overseas*** – On Jan. 22, 2008, Green Supply, Inc., was sentenced in the Eastern District of Missouri to two years probation, a $17,500 fine and an $800 special assessment after pleading guilty in Nov. 2007 to export control violations involving the illegal export of controlled night vision systems. The company was charged via information on Nov. 2, 2007. The investigation was conducted by ICE and BIS.

- ***Firearms to Canada*** – On Jan. 11, 2008, in the Southern District of Florida, defendants Gary Roach and Laron Frazer were convicted on international firearms trafficking charges. The defendants were charged on July 26, 2007, for their role in a scheme in which they used straw purchasers to obtain handguns in Florida, Alabama, and Georgia. They then smuggled the guns to Canada in the door panels of rental cars. This case was investigated by the ATF and ICE.

- ***Military Amplifiers to China*** – On Dec. 19, 2007, Ding Zhengxing, Su Yang and Peter Zhu were

indicted in the Western District of Texas for Arms Export Control Act violations in connection with an alleged plot 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 in January 2008 after they traveled to Saipan to take possession of the amplifiers. Peter Zhu, of Shanghai Meuro Electronics Company Ltd., in China, remains at large. The case was investigated by ICE.

- ***Petrochemical Valves to Iran and Iraq*** – On Dec. 17, 2007, Andrew Freyer was sentenced to 17 months in prison and ordered to pay a $10,000 criminal fine for his part in a conspiracy to export U.S.-origin valves to Iran via Australia. On Aug. 15, 2007, Freyer was convicted at trial of one count of aiding and abetting. On Oct. 15, 2007, Sharon Doe, Inside Sales Manager for Crane Pacific Valves in California, was sentenced to three years probation after pleading guilty in Jan. 18, 2007 for her role in the export of petrochemical valves to Iran and Iraq through Australia in order to avoid the Export Administration Regulations. Both Freyer and Doe was charged on Dec. 1, 2006. This investigation was conducted by BIS.

- ***Military Night Vision Goggles Illegally Exported Overseas*** – On Dec. 11, 2007, Jerri Stringer was sentenced to 48 months of imprisonment and three years of supervised release in the Northern District of Florida after pleading guilty to several violations in connection with a conspiracy with her son, former U.S. Air Force Staff Sgt. Leonard Allen Schenk, to steal restricted military night vision goggles, aviation helmets, and other equipment from the Air Force and sell them to overseas buyers. On Dec. 6, 2007, Schenk was sentenced to 235 months of imprisonment and three years of supervised release after pleading guilty to a 21-count indictment alleging the sale of stolen military equipment overseas and attempting to hire an undercover agent to kill a potential government witness. Schenk and Stringer were charged in the superseding indictment brought on Aug. 21, 2007. This investigation was conducted by ICE.

- ***Military Night Vision Technology to China*** – On Dec. 3, 2007, Philip Cheng was 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 pleaded guilty on Oct. 31, 2006, to brokering the illegal export of Panther-series infrared camera, a device which makes use of "night vision" technology. He was indicted on June. 3, 2004. The technology used in the device was controlled for national security reasons by the United States Department of State. The case was the result of a joint investigation by ICE, the FBI, the Department of Commerce, and the IRS.

- ***Fighter Jet Components to Germany*** – On Nov. 30, 2007, Murray Rinzler and his company World Electronics, Inc, were sentenced in the District of Connecticut to a criminal fine of $20,000 after pleading guilty on March 26, 2007 to charges that they conspired to violate the Arms Export Control Act by sending F-14 fighter jet components and other military items to Germany. Rinzler was also sentenced to two years probation. Both defendants were charged via information on March 26, 2007. This investigation was conducted by ICE, DCIS and BIS.

- ***Military Night Vision Equipment to Hizballah*** – On Nov. 29, 2007, Fawzi Assi, a former resident of Dearborn, Michigan, pleaded guilty to providing material support to Hizballah, a designated foreign terrorist organization. Mr. Assi admitted that, on July 13, 1998, he attempted to board an airplane at Detroit Metro Airport on an international flight for Lebanon with two Boeing global positioning satellite modules, night vision goggles and a thermal imaging camera. He was attempting to deliver these items to a person in Lebanon, who was purchasing the equipment for Hizballah. Shortly after his arrest in 1998, Assi was ordered released from custody during a hearing in which the government sought to have him detained. He fled to Lebanon and remained there until May 2004 when he returned to the United States and was arrested again. The case was investigated by the FBI and ICE

and was prosecuted in the Eastern District of Michigan.

- ***F-14 Fighter Jet Components and Other Military Items to Iran*** – On Nov. 20, 2007, a grand jury in the Southern District of New York returned an indictment charging Yousef Boushvash with violating the Arms Export Control Act, smuggling, conspiracy to commit money laundering and other violations in connection with his alleged acquisition of F-14 military fighter jet components and other military parts from the United States for export to Iran. The grand jury later returned two superseding indictments against Boushvash adding new offenses. According to the charges, Boushvash operated a company in Dubai, United Arab Emirates, called Glasgow International LLC which served as a hub for his illegal arms deals. Boushvash and his co-conspirators allegedly contacted numerous suppliers in the U.S. via e-mail and had them illegally export military components to the UAE, Thailand, and other locations, for ultimate transshipment to Iran. Boushvash had been arrested by Hong Kong authorities on Oct. 29, 2007 in Hong Kong pursuant to a provisional warrant issued by the Southern District of New York. The Justice Department commenced extradition proceedings to bring Boushvash to New York. On April 11, 2008, days before the extradition hearing was scheduled to begin in Hong Kong, authorities in Hong Kong terminated the proceeding and released Boushvash from custody. Boushvash currently is a fugitive from justice and has been placed on Interpol's list of wanted suspects. Three of Boushvash's U.S. suppliers have been convicted in related cases. Lawrence Davis and Gwendolyn Douglas and George Frank Myles Jr. have all pleaded guilty in the Southern District of New York. This investigation was conducted by ICE and DCIS.

- ***Hawk Missile Batteries to Iran*** – On Nov. 9, 2007, in the Western District of Texas, Robert Caldwell was sentenced to 20 months in prison and two years supervised release for attempting to illegally export to Iran specialized batteries for the Hawk Air Defense Missile system. Caldwell, along with co-defendants, Robert Gibson and Christopher Harold Tappin, were charged for their roles in the export plot on Feb. 2, 2007. Gibson later pleaded guilty and was sentenced to serve a two-year prison term. Tappin remains a fugitive. The case was investigated by ICE.

- ***Military Night Vision Technology to China*** – On Oct. 31, 2007, Bing Xu, of Nanjing, China, was 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 on October 26 from China a day after his Chinese employer wire transferred $14,080 to federal agents as payment for the purchase of the restricted equipment. The investigation was conducted by ICE and the DCIS.

- ***U.S. Stealth Missile Data & Military Secrets to China*** – On Oct. 26, 2007, Noshir Gowadia was 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 U.S, as well as unlawfully possessing classified information, and laundering funds paid to him by the Chinese government for his illegal defense work. The original indictment against Gowadia was returned on Nov. 8, 2005. The investigation was conducted by the FBI, Air Force Office of Special Investigations, IRS, CBP, and ICE.

- ***Pipe Cutting Machines to Iran*** – On Oct. 24, 2007, Roger Unterberger, Muhammad Bhatti, and Go-Trans (North America) Inc., three defendants involved with the investigation of Go-Trans (North American) Inc., were sentenced in the Northern District of Illinois after pleading guilty on Aug. 20, 2007 to making false statements in connection with the attempted export of pipe cutting machines to

Iran via Germany. All were charged by criminal information on Aug. 1, 2007. In addition, on July 31, 2007, Mohammed Meshkin was indicted on one count of violating the International Economic Emergency Powers Act in connection with the case. The investigation was conducted by BIS and ICE.

- ***Nickel Powder to Taiwan*** – On Oct. 11, 2007, Theresa Chang was sentenced to three years probation and to pay a $5,000 criminal fine. One June 21, 2007, Chang pleaded guilty to one count of making false statements related to the export of nickel powder controlled for nuclear proliferation reasons to Taiwan without an export license. The investigation was conducted by BIS.

- ***Tractor Parts to Iran*** – On Oct. 11, 2007, Saied Shahsavarani, President of Tak Components, Inc. was sentenced to three years probation and a $1,000 criminal fine after pleading guilty on June 14, 2007 to one count of aiding and abetting the operation of an unlicensed money transmitting business. Also, on Oct. 11, 2007 Tak Components was sentenced to one year probation and to forfeit $38,016. On June 14, 2007, Tak Components pleaded guilty to 16 counts of violating the International Emergency Economic Powers Act. Tak Components illegally exported a variety of equipment to Iran, falsely claiming they were destined for the United Arab Emirates. Both defendants were charged on June 6, 2007. This investigation was conducted by ICE and BIS.

- ***Illegal Exports of F-4 and F-14 Fighter Jet Components*** – On Oct. 5, 2007, Abraham Trujillo and David Wayne of Ogden, Utah, were charged in the District of Utah with attempting to illegally export components for F-4 and F-14 fighter jets using the Internet. According to the charges, the defendants attempted to illegally export military cable assemblies, wiring harnesses and other restricted components to Canada in 2006 and 2007. Such exports are of particular concern because F-14 components are widely sought by Iran, which is currently the only nation in the world that still flies the F-14 fighter jet. The investigation was conducted by ICE and DCIS.

- ***Products with Nuclear & Missile Applications to Pakistan*** – On Oct. 4, 2007, SparesGlobal, Inc., a Pittsburgh company, was sentenced to pay a $40,000 criminal fine in the Western District of Pennsylvania for conspiring to falsify documents and make false statements about a 2003 illegal export to the United Arab Emirates (UAE) that ultimately ended up in Pakistan. According to court documents, SparesGlobal exported to a trading company in the UAE restricted graphite products that can be used in nuclear reactors and in the nose cones of ballistic missiles. The graphite products were routed to Pakistan. After the shipment, the company attempted to mislead federal investigators when questioned about the shipment and related documents. On July 7, 2007, SparesGlobal, represented by its President, Om Sharma, pleaded guilty. The company was charged via information on April 23, 2007. The investigation was conducted by BIS.

- ***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. The case was investigated by the FBI.

- ***Sensitive Aircraft Components to Iran*** – On Sept. 18, 2007, Aviation Services International, a Netherlands-based aviation services company, its owner, Robert Kraaipoel, and two other Dutch companies, Delta Logistics and TPC, were charged in the District of Columbia with illegally exporting aerospace grade aluminum, aircraft components, and other equipment to Iran and the government of Iran. The complaint alleges that, in 2006 alone, Aviation Services obtained some 290 aircraft-related

components from the U.S. and caused them to be shipped to Iran. Many of these U.S.-origin goods were sent to Iranian government agencies, Iranian procurement agencies or companies doing business in Iran, according to the complaint. The investigation was conducted by BIS, ICE, DCIS and FBI.

- ***Restricted Technology to China*** – On Aug. 1, 2007, Fung Yang, the president of Excellence Engineering Electronics, Inc., pleaded 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. Yang was charged by information on July 31, 2007. The investigation was conducted by BIS and the FBI.

- ***Radios, Ammunition Magazines, Scopes to Designated Terrorist in Philippines*** – On Aug. 1, 2007, Rahmat Abdhir was indicted in the Northern District of California on charges of conspiracy to provide material support to terrorists, providing material support to terrorists, and contributing goods and services to a Specially Designated Global Terrorist. According to the indictment, Rahmat Abdhir communicated frequently with Zulkifli Abdhir, his fugitive brother and a U.S.-specially designated terrorist who operates in the Philippines and is a member of the central command of *Jemaah Islamiyah*. From his home in California, Rahmat allegedly sent his brother money, two-way radios, Colt .45 magazines, binoculars, rifle scopes, batteries and other materials, even as his brother evaded capture and battled Philippine troops. Zulkifli Abdhir was charged in the same indictment with conspiracy to provide material support to terrorists and providing material support to terrorists. The investigation was conducted by the FBI and ICE.

- ***Aircraft Components to Iran*** – On July 30, 2007, Ali Khan, the owner of TurboAnalysis in Phoenix, AZ, was sentenced in the Eastern District of New York to five years probation, a $1.4 million forfeiture, and $100,000 criminal fine in connection with his role in a conspiracy to illegally export aircraft components to Iran. Khan previously pleaded guilty to one count of conspiracy to violate the International Emergency Economic Powers Act in Sept. 2005. He was indicted on May 5, 2004. This investigation was conducted by BIS and ICE.

- ***Sensitive Technology to Prohibited Facility in India*** – July 30, 2007, Samuel Shangteh Peng was charged in the Central District of California with illegally exporting sensitive technology to an entity in India prohibited from receiving such technology due to proliferation concerns. Peng, an international sales manager at a California company, was charged with illegally exporting vibration amplifiers, cable assemblies and vibration processor units in 1999 and 2000 from the U.S. to Hindustan Aeronautics Limited, Engine Division, in India. In 1998, the U.S. government designated this facility in India as an end-user of concern for proliferation reasons. The investigation was conducted by BIS, ICE, and the Naval Criminal Investigative Service (NCIS).

- ***Missiles, Explosives, Arms to Overthrow Government in Laos*** – On June 14, 2007, a grand jury in the Eastern District of California returned an indictment charging 11 defendants with conspiring to overthrow the government of Laos by force and violence. Among other things, the defendants were charged with conspiring to acquire hundreds of assault rifles, Stinger missiles, anti-tank missiles, mines, and C-4 explosives which they intended to ship to safe houses in Thailand and Laos for use in overthrowing the government of Laos. Harrison Ulrich Jack, Vang Pao, Lo Cha Thao, Lo Thao, Yua True Vang, Hue Vang, Chong Yang Thao, Seng Vue, Chue Lo, Nhia Kao Vang, and Dang Vang were charged in the indictment with conspiracy to violate the Arms Export Control Act, conspiracy to violate the Neutrality Act, conspiracy to kill, kidnap, and maim; conspiracy to possess a missile system to destroy aircraft, and other violations. The investigation was conducted by the ATF and FBI.

- ***Missiles, Arms to Terrorists in Colombia and Armed Factions Around the Globe*** – On June 7,

2007, reputed international arms dealer, Monzer Al Kassar, was arrested in Spain and two of his alleged associates, Tareq Mousa El Ghazi and Luis Felipe Moreno Godoy, were arrested in Romania pursuant to a terrorism-related indictment returned in the Southern District of New York. According to the May 29, 2007 indictment, Kassar agreed to sell millions of dollars worth of surface-to-air missiles, rocket-propelled grenade launchers, ammunition, and machine guns to the U.S.-designated terrorist organization, Fuerzas Armadas Revolucionarias de Colombia (FARC), between February 2006 and May 2007. S ince the early 1970s, court documents allege, Kassar has been a ready source of weapons and military equipment for armed factions engaged in violent conflicts around the world, including Nicaragua, Brazil, Cyprus, Bosnia, Croatia, Somalia, Iran, and Iraq, among other countries. The investigation was conducted by the Drug Enforcement Administration (DEA) and the FBI.

- ***F-14 Fighter Jet Components to Iran*** – On May 8, 2007, Reza Tabib was sentenced in the Central District of California to violating the International Emergency Economic Powers Act in connection with his efforts to illegally export military aircraft parts to Iran via associates in Germany and the United Arab Emirates. In 2006, federal agents intercepted maintenance kits for the F-14 fighter jet that Tabib and his wife, Terri Tabib, had sent to Iran. A search of their California home led to the seizure of more than 13,000 aircraft parts as well as various aircraft part "shopping lists" that provided to the couple by an Iranian military officer. Reza Tabib pleaded guilty on June 5, 2006 after being charged in Feb. 2006. His wife Terri pleaded guilty on Dec. 14, 2006. The investigation was conducted by ICE and DCIS.

- ***Controlled Telecommunications Equipment to Cuba*** – On April 25, 2007, LogicaCMG Inc., pleaded guilty in the District of New Hampshire and was sentenced to pay a $50,000 criminal fine for illegally causing goods to be exported to Cuba. In 2001, LogicaCMG's predecessor company, CMG Telecommunications, exported telecommunications equipment controlled for national security reasons to Cuba via Panama without the required export license. The company was charged by information on March 30, 2007. This case was investigated by ICE and BIS.

- ***Military Night Vision Components to India*** – On April 19, 2007, a jury in the Western District of Pennsylvania convicted Electro-Glass Products, a Pennsylvania company, of violating the Arms Export Control Act. Evidence at trial established that Electro-Glass illegally exported 23,000 solder glass performs, which are components of military night vision equipment, to a company in India without the required State Department license. The company was indicted on April 5, 2006. The investigation was conducted by ICE.

- ***Telecommunications Equipment from China to Iraq*** – On April 10, 2007, Andrew Huang, the owner of McAndrew's, Inc, an international export company, pleaded 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. The investigation was conducted by the FBI, ICE, NCIS, IRS and BIS.

- ***Ballistic Helmets to Suriname*** – On March 28, 2007, Alpine Armoring, Inc., a Virginia company, pleaded guilty in the Eastern District of Virginia to the unlicensed export of controlled ballistic helmets to Suriname. Fred Khoroushi, the president and director of Alpine Armoring, also pleaded guilty to making false statements on an export declaration. Both Alpine Armoring and Khoroushi were charged via information on March 27, 2007. The investigation was conducted by BIS, ICE, and DCIS.

- ***$100 Million Penalty for Illegal Exports of Military Night Vision Technology to China,***

Singapore, U.K . -- On March 27, 2007, ITT Corporation, the leading manufacturer of military night vision equipment for the U.S. Armed Forces, agreed to pay a $100 million penalty and admitted to illegally exporting restricted night vision data to China, Singapore, and the United Kingdom in the Western District of Virginia. The company also pleaded 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 of the most advanced night vision systems in the world for the U.S. Armed Forces. The investigation was conducted by DCIS and ICE.

- ***Machine Guns, Arms to Indonesia*** – On Jan. 18, 2007, Hadianto Djuliarso pleaded guilty in the Eastern District of Michigan to conspiracy to violate the Arms Export Control Act and money laundering in a scheme to purchase and illegally export more than $1 million worth of machine guns, sniper rifles and other weapons to Indonesia. According to court documents, Djuliarso also made inquiries about purchasing Sidewinder missiles and strafing ammunition for illegal export to Indonesia. Three other defendants, Ibrahim Bin Amran, Ignatius Soeharli, and David Beecroft, have pleaded guilty in this case. The investigation was conducted by ICE and DCIS.

- ***U.S. Anti-Submarine Torpedo Technology to South Korea*** – On Dec. 21, 2006, Stuart Choi pleaded guilty to an export violation for his role in a scheme to illegally export U.S. anti-submarine torpedo technology to South Korea. The technology was destined for the South Korean "Blue Shark" anti-submarine torpedo program made public during the summer of 2006. This investigation was conducted by ICE.

- ***Stolen Trade Secrets to Chinese nationals*** – On Dec. 14, 2006, Fei Ye and Ming Zhong pleaded guilty in the Northern District of California 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. They were first indicted on Dec. 4, 2002. The investigation was conducted by ICE, FBI and CBP.

- ***Sensitive Technology to Iranian National*** – On Dec. 5, 2006, Seyed Rohani Eftekhari pleaded guilty in the Western District of Texas to attempting to purchase a "guided wave" scanning device with the intent of providing the unit to a third party from Iran without the required U.S. government license. He was charged on Oct. 4, 2006. The investigation was conducted by ICE and the FBI.

- ***Technology with Nuclear Applications to Iran*** – On Nov. 30, 2006, Juan Sevilla, sales director of United Calibration Corporation in California, was sentenced in the Northern District of Illinois for attempting to illegally export to Iran machinery and software to measure the tensile strength of steel in violation of the U.S. embargo. The technology is on the Nuclear Supplier's Group "Watch List" as a commodity that can make a contribution to nuclear activities of concern. Sevilla was indicted on March 1, 2005 and pleaded guilty on Sept. 14, 2005. The investigation was conducted by BIS and ICE.

- ***Rifle Scopes, Weapons to Iran*** – On Nov. 22, 2006, Fereidoon Karlman was arrested in the Eastern District of Michigan after authorities found rifle scopes, laser range finding binoculars, stun guns and other prohibited items in luggage for his trip to Iran. He pleaded guilty on Nov. 15, 2007 and was later sentenced on March 18, 2008. The investigation was conducted by ICE.

- ***Missile Technology / Military Accelerometers to Iran*** – On Nov. 13, 2006, officials with the Royal Thai Police arrested Jamshid Ghassemi in Bangkok, Thailand, pursuant to a provisional U.S. arrest

warrant. Ghassemi and a co-conspirator, Aurel Fratila, had been indicted on October 17, 2006 in the Southern District of California on charges of conspiracy to violate the Arms Export Control Act, conspiracy to launder money, and money laundering. According to the indictment, the defendants attempted to illegally export military gyroscopes and military accelerometers suitable for ballistic missile guidance, as well as spacecraft navigation and control systems, to Romania for ultimate transshipment to Iran. Ghassemi was released by Thai authorities in Sept. 2008 after the U.S. extradition request was denied. He remains a fugitive. This investigation was conducted by ICE and DCIS.

- ***Military Weapons Scopes to China*** – On Oct. 25, 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. He pleaded guilty on Dec. 11, 2006. The investigation was conducted by DCIS, BIS, and ICE.

- ***U.S. Military Vehicles to the Middle East*** – On Oct. 24, 2006, Ronald Wiseman, a former Defense Reutilization and Marketing Service (DRMS) official, was sentenced in the District of Columbia for illegally selling militarized vehicles to individuals in Middle East nations. A second former DRMS official, Gayden Woodson, pleaded guilty the same day in connection with the scheme. Both were charged on May 5, 2005. The case was investigated by ICE, DCIS and the Defense Logistics Agency.

- ***Terrorist Transactions, Computer Exports to Libya and Syria*** – On Oct. 13, 2006, sentences were handed down in the Northern District of Texas against Infocom Corporation and Bayan Elashi, Ghassan Elashi and Basman Elashi in connection with prior convictions at trial for dealing in the funds of a Specially Designated Terrorist, a high-ranking official of the terrorist organization, Hamas, and conspiracy to export computers and computer equipment to Libya and Syria. The investigation was conducted by FBI, BIS, ICE, IRS and members of the North Texas Joint Terrorism Task Force.

- ***Aircraft Parts to Iran*** – On Oct. 13, 2006, Ernest Koh, doing business as Chong Tek, was sentenced in the Eastern District of New York to jail after his conviction at trial for obtaining components that can be used in C-130 military transport planes and P-3 Naval aircraft, and diverting those parts to Malaysia for ultimate transshipment to Iran. In total, the government found that Koh illegally exported roughly $2.6 million in aircraft parts to Iran. Koh was first charged on Oct. 26, 2005. The investigation was conducted by BIS and ICE.

- ***Industrial Furnace to Missile Institute in China*** – On Oct. 4, 2006, William Kovacs, the owner and president of Elatec Technology Corporation in Massachusetts, was sentenced in the District of Columbia to 12 months 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. Kovacs and Elatec pleaded guilty to conspiring to violate export laws on May 28, 2004. They were first charged on Nov. 13, 2003. An associate, Stephen Midgley, separately pleaded guilty on Jan. 10, 2005, to making false statements in export documents. The investigation was conducted by BIS and ICE.

Press Release

###

08-959

Pages 133 through 139 redacted for the following reasons:
- -
NSD FOIA 09-037-0006
DIRECT RESPONSE

RELEASE

Department of Justice

FOR IMMEDIATE RELEASE
APRIL 2009
WWW.USDOJ.GOV

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

FACT SHEET: MAJOR U.S. EXPORT ENFORCEMENT PROSECUTIONS (FISCAL YEAR 2006 TO THE PRESENT)

Below is a snapshot of some of the major export and embargo-related criminal prosecutions handled by the Justice Department since October 2006. These cases resulted from investigations by the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE), the Federal Bureau of Investigation (FBI), the Department of Commerce's Bureau of Industry and Security (BIS), the Pentagon's Defense Criminal Investigative Service (DCIS), and other law enforcement agencies. This list of cases is not exhaustive and only represents select cases.

- ***Rocket Propulsion Systems, Engines and Technology to South Korea*** – On April 15, 2009, Juwhan Yun, a.k.a. J.W. Yun, a U.S. citizen of Korean origin, was arrested in Fort Lauderdale, Fla., for conspiring to illegally export defense articles to South Korea, specifically RD 180 rocket propulsion systems, engines, and technology that are on the U.S. Munitions List and the Missile Technology Control Regime Annex. A criminal complaint filed in the Southern District of Florida alleges that Yun was attempting to purchase these rocket materials for a company working on the Korean Satellite Launch Vehicle project and which was previously involved in developing Korea's KOMPSAT-1 satellite. Yun was previously convicted in May 1989 of conspiracy to violate the Arms Export Control Act in connection with an effort to export sarin nerve gas bombs to Iran. He was sentenced to 30 months in federal prison in 1989. He was released from federal prison in March 1991 and was debarred by the State Department as a result of his conviction. This investigation was conducted by ICE and DCIS.

- ***Trade Secrets to China*** – On April 10, 2009 Yan Zhu, a Chinese citizen in the U.S. on a work visa, was arrested in the District of New Jersey on charges of theft of trade secrets, conspiracy, wire fraud, and theft of honest services fraud in connection with a plot to steal software from his former U.S. employer and sell a modified version to the Chinese government after he was fired. Zhu was employed as a senior environmental engineer from May of 2006 until his termination in July of 2008. Zhu worked for a comprehensive multi-media environmental information management portal that developed a proprietary software program for the Chinese market which allows users to manage air emissions, ambient water quality, and ground water quality. This investigation was conducted by the FBI.

- ***Restricted Technology to China*** – On April 7, 2009, Fu-Tain Lu was arrested in San Francisco pursuant to an April 1, 2009 indictment in the Northern District of California charging him with lying to federal agents and conspiring to illegally export restricted microwave amplifier technology to China. According to the indictment, Lu, and the two companies he founded, Fushine Technology, Inc., of Cupertino, Calif., and Everjet Science and Technology Corporation, based in China, conspired to export sensitive microwave amplifier technology that was restricted for national security reasons to China without first obtaining a Commerce Department license.

This investigation was conducted by the Department of Commerce (BIS), the FBI, ICE, and U.S. Customs and Border Protection.

- ***Rocket / Space Launch Technical Data to China*** – On April 7, 2009, Shu Quan-Sheng, a native of China, naturalized U.S. citizen and PhD physicist, was sentenced to 51 months in prison for illegally exporting space launch technical data and defense services to the People's Republic of China (PRC) and offering bribes to Chinese government officials. Shu pleaded guilty on Nov. 17, 2008, in the Eastern District of Virginia to a three-count criminal information. He was arrested on Sept. 24, 2008. He was the President, Secretary and Treasurer of AMAC International, a high-tech company located in Newport News, Va., and with an office in Beijing, China. Shu provided the PRC with assistance in the design and development of a cryogenic fueling system for space launch vehicles to be used at the heavy payload launch facility located in the southern island province of Hainan, PRC. The Hainan facility will house launch vehicles designed to send space stations and satellites into orbit, as well as provide support for manned space flight and future lunar missions. Shu also illegally exported to the PRC technical data related to the design and manufacture of a "Standard 100 M3 Liquid Hydrogen (LH) 2 Tank. In addition, Shu offered approximately $189,300 in bribes to government officials with the PRC's 101 Institute to induce the award of a hydrogen liquefier project to a French company he represented. In January 2007, the $4 million hydrogen liquefier project was awarded to the French company that Shu represented. This investigation was conducted by the FBI, ICE, BIS and DCIS.

- ***Military Aircraft Components to Iran*** – On April 2, 2009, eleven defendants were indicted in the Southern District of Florida on charges of participating in a conspiracy to export U.S.-made military aircraft parts to Iran. On April 3, 2009, federal agents arrested defendant Baktash Fattahi, an Iranian national and legal U.S. resident, at his residence in Lancaster, Calif. The other ten defendants charged in the indictment are Amir Hosein Atabaki, an Iranian national; Mohammad Javad Mohammad Esmaeil, an Iranian national; Abbas Haider, an Indian citizen residing in Dubai; Mohammed Javid Yahya Saboni, an Iranian national residing in Dubai; Reza Zahedi Pour, an Iranian national; Mahdi Electronic Trading Co, an Iranian business; Planet Commercial Brokerage, a Dubai business; Raht Aseman Co, Ltd, an Iranian business; Sahab Phase, an Iranian business; and Sea Speed UAE, a Dubai business. According to the indictment, the defendants conspired to and did export 13 different types of military aircraft parts to Iran by way of Dubai, United Arab Emirates. Among the aircraft parts the defendants are alleged to have obtained and illegally shipped to buyers in Iran are parts for the F-5 ("Tiger") Fighter Jet, the Bell AH-1 ("Cobra") Attack Helicopter, the CH-53 Military Helicopter, the F-14 ("Tomcat") Fighter Jet, and the UH-1 ("Huey") Military Helicopter. According to the Indictment, defendants in Iran sent orders by email to a co-conspirator in Novato, Calif., for specific aircraft parts. The co-conspirator in Calif. then requested quotes, usually by e-mail, from another co-conspirator in Plantation, Fla., and made arrangements with that co-conspirator in Plantation for the sale and shipment of the parts to one of several defendants in Dubai. From Dubai, the parts were then shipped on to Iran. This investigation was conducted by ICE, DCIS, Diplomatic Security Service, with assistance from OFAC and State Department's Directorate of Defense Trade Controls.

- ***Fighter Jet and Military Helicopter Components to Iran*** – On April 2, 2009, Traian Bujduveanu pleaded guilty in the Southern District of Florida to conspiracy to illegally export military and dual-use aircraft components to Iran. Bujduveanu appeared on behalf of himself and his now defunct corporation, Orion Aviation Corp., in federal court to announce his guilty plea. Bujduveanu's co-defendant, Hassan Keshari, and his corporation, Kesh Air International, pleaded guilty in January 2009 to charges of conspiring to illegally export military and commercial aircraft components to Iran. On July 3, 2008, Keshari, Kesh Air International, as well as

Bujduveanu, and his company Orion Aviation, were indicted for their participation in a conspiracy to export U.S.-made military and dual-use aircraft parts to Iran. On June 20, 2008, agents arrested Keshari at Miami International Airport as he walked off a flight from Atlanta. Bujduveanu was arrested at his Plantation, Florida, home on June 21, 2008. Since August 2006, Keshari and Bujduveanu have allegedly procured U.S.-made military aircraft parts for buyers in Iran and have illegally shipped the parts to a company in Dubai, UAE, for shipment to buyers in Iran. Keshari allegedly received the orders for specific parts by e-mail from buyers in Iran. Keshari then requested quotes, usually by e-mail, from Bujduveanu and made arrangements with Bujduveanu for the sale and shipment of the parts to a company in Dubai. From Dubai, the parts were then shipped on to Iran. Keshari and Bujduveanu are alleged to have obtained and illegally shipped to buyers in Iran parts for the CH-53 military helicopter, the F-14 Tomcat fighter jet, and the AH-1 attack helicopter. Keshari is also alleged to have requested quotes for other parts for other military aircraft, including F-4 Phantom aircraft. This investigation was conducted by BIS, ICE, and DCIS.

- ***Military Aircraft Parts to Israel*** – On April 2, 2009, Stuart Wax pleaded guilty in the District of Connecticut to a one-count criminal information charging him with making a false statement in an export control document. Wax entered the plea both for himself and on behalf of his company, M.M.M. Wheels, Inc. In 2003, Wax exported parts used in the F-4 fighter jet to be sent to a company in Israel without the required license from State Department. Wax indicated on the shipping documents that the box contained "plumbing parts for repair," although he knew the contents actually were parts for military aircraft. This investigation was conducted by ICE, DCIS, and BIS agents.

- ***Thermal Imaging Cameras to South Korea*** – On March 25, 2009, David Lee plead guilty in the Northern District of Illinois to a one count indictment charging that he illegally exported thermal imaging cameras to South Korea without obtaining the required export license. Lee, the owner of Lucena Technology, Inc., an export company in Park Ridge, Ill., exported seven thermal imaging cameras to South Korea in June 2007 without obtaining the required U.S. Department of Commerce export license. Under the terms of the plea agreement, Lee agreed to forfeit $59,500 which represents the proceeds from the sale of the cameras. Lee was originally indicted on Dec. 16, 2008. The investigation was conducted by BIS and U.S. Customs and Border Protection.

- ***Aircraft Engines and Components to Iranian Military*** – On March 24, 2009, a 25-count indictment was unsealed in the District of Columbia charging Mac Aviation Group, a trading company in Ireland, and three of its officers with purchasing aircraft engines and components from U.S. firms and illegally exporting these components to Iran via Malaysia and the United Arab Emirates. Among the alleged recipients of these goods was the Iran Aircraft Manufacturing Industrial Company (HESA), a military entity designated by the U.S. for its role in Iran's nuclear and ballistic missile program, as well as Iran Aircraft Industries (IACI). The three Mac Aviation officers charged in the indictment, which was filed on July 22, 2008, are Thomas McGuinn, his son, Sean McGuinn, and Sean Byrne. According to the indictment, the defendants purchased 17 aircraft engines from Rolls-Royce in Indiana and caused them to be exported to a publishing company in Malaysia, and later shipped on to HESA in Iran. The indictment also alleges that the defendants purchased 50 aircraft components known as "5th Stage vanes" from the United States and illegally exported them to Iran, and also obtained various U.S.-origin aircraft bolts, which they routed through a trading company in the United Arab Emirates to Iran. The defendants are alleged to have worked with Hossein Ali Khoshnevisrad and his Tehran business, Ariasa, AG, in purchasing some of these components for Iran. This case was investigated by ICE and BIS.

- ***Sensitive U.S. Technology to Iranian Missile & Nuclear Entities*** -- On March 20, 2009, Iranian national and resident Majid Kakavand was arrested overseas pursuant to a provisional U.S. arrest warrant issued in the Northern District of California. A March 6, 2009 criminal complaint charges him with overseeing an international network that allegedly purchased thousands of military and commercial items from U.S. companies and illegally exported these goods to Iran via Malaysia. The alleged recipients of these goods included two Iranian military entities designated by the United States for their role in Iran's nuclear and ballistic missile program. According to the affidavit filed in support of the complaint, Kakavand served as director of a company in Malaysia called Evertop Services Sdn Bhd, that he and others created to procure goods from the United States and Europe for export to Iran. Evertop Services' primary customers in Iran were two Iranian military entities, Iran Electronics Industry (IEI), and Iran Communication Industries (ICI), both of which were designated in 2008 by the United States for their role in Iran's nuclear and ballistic missile programs. Furthermore, IEI was listed by the European Union as an entity linked to Iran's proliferation-sensitive nuclear activities or Iran's development of nuclear weapon delivery systems. Using Evertop Services, Kakavand allegedly purchased products for Iran from U.S. companies in several states, including California, Alabama, Florida, Washington, and New Jersey. Kakavand has allegedly exported more than 30 shipments of goods from the United States to Iran since February 2006. These shipments contained electronic and avionic components, including capacitors, spectrometers, resistors, sensors, connectors, and airborne antennae. Kakavand allegedly concealed from the U.S. companies that the ultimate end-users of these products were in Iran, and at no time did he have a license to export or re-export goods to Iran. For example, in one transaction, Kakavand allegedly purchased 41,900 radiall connectors from a company in California and, in January 2008, wired $51,425 to the firm as payment for the goods. The affidavit indicates that these goods were exported from the United States to Evertop Services in Malaysia, then re-exported to ICI in Iran. In other transactions spelled out in the affidavit, Kakavand used similar techniques to illegally export sensors, inductors and other materials to Iran. This investigation was conducted by BIS and ICE.

- ***Carbon-Fiber Material with Rocket & Spacecraft Applications to China*** – On March 20, 2009, Jian Wei Ding pleaded guilty in the District of Minnesota to one count of conspiracy to violate the Export Administration Regulations. Ding was the last of three defendants in this case to plead guilty to exporting sensitive carbon-fiber material from the United States to Singapore, Hong Kong and the People's Republic of China in violation of the export regulations of the United States. The other two defendants, Ping Cheng and Kok Tong Lim, also pleaded guilty to one count of conspiracy. Cheng entered his plea on Feb. 13, 2009 and Lim entered his plea on March 9, 2009. All three men were indicted on Oct. 28, 2008 for conspiring to illegally export to China controlled carbon-fiber material with applications in aircraft, rockets, spacecraft, and uranium enrichment process. The intended destination for some of the materials was the China Academy of Space Technology, which oversees research institutes working on spacecraft systems for the PRC government. For national security, nuclear proliferation and antiterrorism reasons, the U.S. government requires a license to export these carbon-fiber materials. Jian Wei Ding was a resident of Singapore and owned or was a affiliated with various Singaporean import/export companies, including Jowa Globaltech Pte Ltd, FirmSpace Pte Ltd, and Far Eastron Co. Pte Ltd. Kok Tong Lim was a resident resident of Singapore and once was affiliated with FirmSpace, Pte Ltd. Ping Cheng was a resident of New York and the sole shareholder of Prime Technology Corporation. This investigation was conducted by ICE and BIS.

- ***Missiles & Other Arms to Colombian Terror Organization*** – On March 17, 2009, Palestinian born businessman Tareq Mousa al-Ghazi was convicted in the Southern District of New York on charges that he conspired with Syrian arms dealer, Monzer Al-Kassar, and others in a plot to sell

surface-to-air missiles, 4,000 grenades, and nearly 9,000 assault rifles to the Fuerzas Armadas Revolucionarias de Colombia, or FARC, a designated terrorist organization in Colombia. Al-Ghazi was found guilty of conspiracy to murder U.S. officers and employees, conspiracy to acquire and export anti-aircraft missiles, and conspiracy to provide material support to terrorists. Al-Ghazi's co-defendants, Monzer al-Kassar and Luis Felipe Moreno Godoy, were both convicted at trial on Nov. 20, 2008 in connection with the same conspiracy and were sentenced on Feb. 24, 2009 to 30 years imprisonment and 25 years imprisonment, respectively. In June 2007, Al Kassar was arrested in Spain, while Moreno and El Ghazi were arrested in Romania pursuant to a May 29, 2007 indictment alleging that they agreed to sell millions of dollars worth of surface-to-air missiles, rocket-propelled grenade launchers, ammunition, and machine guns to the FARC, between February 2006 and May 2007. Al Kassar also offered to send 1,000 men to fight with the FARC against U.S. military officers in Colombia. On June 13, 2008, Al Kassar arrived in New York after being extradited from Spain. Since the early 1970s, Al Kassar has been a source of weapons and military equipment for armed factions engaged in violent conflicts around the world. Some of these factions have included known terrorist organizations, such as the Palestinian Liberation Front, the goals of which included attacking United States interests and United States nationals. The investigation was conducted by the Drug Enforcement Administration, Spanish National Police and Romanian Border Police.

- ***Aircraft Engines and Advanced Surveillance Cameras to Iranian Military*** -- On March 14, 2009, Hossein Ali Khoshnevisrad was arrested in San Francisco pursuant to a sealed criminal complaint charging him and his Tehran-based business, Ariasa, AG, with purchasing helicopter engines and advanced aerial cameras for fighter bombers from U.S. firms and illegally exporting them to Iran using companies in Malaysia, Ireland and the Netherlands. Among the alleged recipients of these U.S. goods was an Iranian military firm that has since been designated by the United States for being owned or controlled by entities involved in Iran's nuclear and ballistic missile program. The criminal complaint, which was filed under seal in the District of Columbia on Aug. 1, 2008 and unsealed on March, 16, 2009, charges Khoshnevisrad and Ariasa with two counts of unlawfully exporting U.S. goods to Iran and two counts of conspiracy to unlawfully export U.S. goods to Iran in violation of the International Emergency Economic Powers Act. According to the complaint, from Jan. 2007 through Dec. 2007, Khoshnevisrad and Ariasa caused a trading company in Ireland to purchase 17 model 250 turbo-shaft helicopter engines from Rolls-Royce Corp. in Indiana for $4.27 million. The Irish Trading company concealed from Rolls-Royce the end user of the engines, and arranged for them to be exported from the U.S. to a purported "book publisher" in Malaysia, and later shipped to Iran. Among the recipients in Iran was the Iran Aircraft Manufacturing Industrial Company, known as HESA, which was designated by the United States for being controlled by Iran's Ministry of Defense and Armed Forces Logistics and providing support to the Iranian Revolutionary Guard Corps. According to the complaint, Khoshnevisrad and Ariasa also caused to be exported to Iran several aerial panorama cameras from the United States. These cameras were designed for the U.S. Air Force for use on bombers, fighters and surveillance aircraft, including the F-4E Phantom fighter bomber, which is currently used by the Iranian military. According to the affidavit, in 2006, Khoshnevisrad instructed a Dutch aviation parts company to place an order for these cameras with a U.S. company located in Pennsylvania and to ship them to an address in Iran. According to the affidavit, the Dutch company ordered the aerial panorama cameras from the Pennsylvania firm, falsely stating that the Netherlands would be the final destination for the cameras. This investigation was conducted by BIS, FBI, ICE and DCIS.

- ***Military & Commercial Aircraft Components to Iran*** – On March 13, 2009, in the Eastern District of New York, Laura Wang-Woodford, a U.S. citizen who served as a director of Monarch Aviation Pte, Ltd. ("Monarch"), a Singapore company that imported and exported military and

commercial aircraft components for more than 20 years, pled guilty to conspiring to violate the U.S. trade embargo by exporting controlled military and commercial aircraft components to Iran. Wang-Woodford was arrested on Dec. 23, 2007, at San Francisco International Airport after arriving on a flight from Hong Kong, and has remained incarcerated since. She and her husband, Brian D. Woodford, a U.K. citizen who served as chairman and managing director of Monarch, were originally charged in a 20-count indictment on January 15, 2003. Brian Woodford remains a fugitive. A superseding indictment charging Wang-Woodford with operating Jungda International Pte. Ltd ("Jungda"), a Singapore-based successor to Monarch, was returned on May 22, 2008. According to the superseding indictment, the defendants exported controlled U.S. aircraft parts from the U.S. to Monarch and Jungda in Singapore and Malaysia and then re-exported those items to companies in Tehran, Iran, without obtaining the required U.S. government licenses. The defendants also falsely listed Monarch and Jungda as the ultimate recipients of the parts on export documents filed with the U.S. government. The aircraft parts illegally exported to Iran include aircraft shields, shears, "o" rings, and switch assemblies, as well as U.S. military aircraft components, designed for use in Chinook military helicopters. At the time of her arrest, Wang-Woodford possessed catalogues from a Chinese company, the China National Precision Machinery Import and Export Corporation ("CPMIEC"), containing advertisements for surface-to-air missile systems and rocket launchers. CPMIEC has been sanctioned by the Treasury Department as a specially designated Weapons of Mass Destruction proliferator, based, in part, on CPMIEC's history of selling military hardware to Iran. The investigation was conducted by BIS and ICE.

- ***Miniature Unmanned Aerial Vehicle Components to China*** -- On March 12, 2009, a federal grand jury in the District of Columbia returned an indictment charging Yaming Nina Qi Hanson, her husband Harold Dewitt Hanson (an employee at Walter Reed Army Medical Center), and a Maryland company, Arc International, LLC, with illegally exporting miniature Unmanned Aerial Vehicle (UAV) Autopilots to a company in the People's Republic of China. The UAV components are controlled for export to China for national security reasons. According to court documents, beginning in 2007, the Hansons began attempting to acquire the autopilots from a Canadian manufacturer in order to re-export them to Xi'an Xiangyu Aviation Technical Group in China. Qi Hanson initially represented that the autopilots would be used for a model airplane civilian flying club in China. When Canadian company officials questioned the utility of autopilots – designed for use on unmanned aircraft – for flying club hobbyists, Qi Hanson claimed that autopilots would be used on US aircraft to record thunderstorm and tornado developments and ice-pack melting rates in the arctic. On or about August 7, 2008, after having fraudulently taken delivery of 20 of these autopilots (valued at $90,000), Qi Hanson boarded a plane in the United States bound for Shanghai, and hand-delivered the items to Xi'an Xiangyu Aviation Technical Group in China. The investigation was conducted by BIS and FBI.

- ***3,500 Military Night Vision Goggles to Iranian military*** – On March 6, 2009, Shahrazad Mir Gholikhan was sentenced in the Southern District of Florida to 63 months in prison for brokering defense articles to Iran and other export violations in connection with an effort by her and her husband, Mahmoud Seif, to illegally procure 3,500 sets of Generation III military night vision goggles from the United States for Iran's military and police forces. Gholikhan was convicted of the charges on Dec. 19, 2008. Gholikhan and her husband were first arrested in 2004 in Vienna, Austria, after a meeting with undercover law enforcement officials in which they received the first sample shipment of U.S. night vision goggles destined for Iran. After her arrest, Gholikhan told authorities that she and her husband were not allowed to transport the items from Austria to Iran, but that the Iranian Embassy in Austria was to organize the shipment of night vision goggles to Iran. Austrian authorities subsequently released the couple and they returned to Iran. Seif remains a fugitive. Gholikhan was arrested by U.S. authorities in December 2007 upon her arrival

in the United States. She later pleaded guilty to one count of conspiracy. However, she subsequently withdrew the plea after a dispute over her sentence and represented herself at a new trial in 2008, where she was convicted of three of six counts. This investigation was conducted by ICE, DCIS, and Austrian law enforcement.

- ***Amplifiers & Missile Target Acquisition Technology to China*** – On March 5, 2009, Joseph Piquet, the owner and President of AlphaTronX, a company in Port St. Lucie, Fla., that produces electronic components, was convicted in the Southern District of Florida of seven separate counts arising from a conspiracy to purchase military electronic components from Northrop Grumman Corporation, and to ship them to Hong Kong and the People's Republic of China without first obtaining required export licenses under the Arms Export Control Act and the International Emergency Economic Powers Act. Among those items involved in the conspiracy were high-power amplifiers designed for use by the U.S. military in early warning radar and missile target acquisition systems, as well as low noise amplifiers that have both commercial and military use. Piquet was first indicted on June 5, 2008, along with his company, AlphaTronX, Inc, as well as Thompson Tam, and Ontime Electronics Technology Limited. Tam is a director of Ontime Electronics, an electronics company in China. This investigation was conducted by BIS and ICE.

- ***Military Night Vision Technology to China*** – On Feb. 24, 2009, Bing Xu, of Nanjing, China, pleaded guilty in the District of New Jersey to conspiracy to illegally export military-grade night vision technology to China. Xu, a manager at Everbright Science and Technology, Ltd, a company in Nanjing, admitted that he conspired with others at Everbright to purchase certain night-vision technology from a company in the United States, which required a license from the State Department for export. Xu admitted that he and others at Everbright first attempted to obtain the necessary export license for the night-vision equipment. When the license application was denied by the Department of State, Xu agreed with others at Everbright to take steps to export the night-vision optical equipment illegally. Xu has been in custody since his arrest in on October 2007 pursuant to a criminal complaint. Xu arrived in New York on Oct. 26, 2007 from China a day after his Chinese employer wire transferred $14,080 to federal agents as payment for the purchase of the restricted equipment. The investigation was conducted by ICE and the DCIS.

- ***Thermal Imaging Technology to China*** – On Feb. 23, 2009, Zhi Yong Guo, a resident of Beijing, was convicted at trial in the Central District of California of two federal charges related to a plot to procure and export thermal-imaging cameras to the People's Republic of China without obtaining the required export licenses. The charges relate to ten cameras concealed in luggage destined for China in April 2008. The export of the thermal-imaging cameras to China are controlled by the Department of Commerce for national security and regional stability reasons because of their use in a wide variety of civilian and military applications. Previously in this case, Tah Wei Chao, of Beijing, China, pleaded guilty on July 16, 2008, to three felony counts: conspiracy, and two counts of exporting and/or attempting to export restricted items. In March 2008, Chao ordered 10 thermal-imaging cameras from FLIR Systems, Inc. for $53,000. Representatives from FLIR Systems repeatedly warned Chao that the cameras could not be exported without a Commerce Department license. Both Chao and Guo were arrested at Los Angeles International Airport in April 2008 after authorities recovered the 10 cameras that had been hidden in their suitcases, stuffed in shoes and concealed in clothing. In addition to the 10 cameras intercepted by federal authorities in April 2008, Chao admitted that, acting at the behest of Guo, he shipped three cameras to China in October 2007. The evidence at trial showed that Guo, an engineer and a managing director of a technology development company in Bejing, directed Chao to obtain the cameras for Guo's clients, the Chinese Special Police and the Special Armed Police. This case is the product of an investigation by the Export and Anti-proliferation

Global Law Enforcement (EAGLE) Task Force in the Central District of California, including BIS, ICE, FBI, CBP, DSS, and TSA.

- ***Chemical Purchasing Software to Iran*** – On Feb. 13, 2009, in the Eastern District of Pennsylvania, after a seven-day jury trial, Ali Amirnazmi, was found guilty of conspiracy to violate the International Emergency Economic Powers Act (IEEPA); three counts of violating IEEPA, three counts of making false statements; and three counts of bank fraud. Amirnazmi was acquitted of conspiracy to act and acting as an unregistered agent of the government of Iran, as well as one IEEPA charge. Amirnazmi, the owner of Trantech Consultants, Inc., in Pa., was charged by superseding indictment in October 2008 with crimes relating to his participation from 1996 to July 2008 in illegal business transactions and investments with companies located in Iran, including companies controlled in whole or in part by the government of Iran, as well as lying to federal officials about those transactions, and bank fraud. Amirnazmi is a chemical engineer who, among other things, licensed to Iranian companies the use of a proprietary database and software system that he had developed. The software was designed to help buyers around the globe locate the best prices for various chemicals. Amirnazmi, a citizen of both the United States and Iran, was first indicted on July 25, 2008. The case was investigated by the FBI and IRS.

- ***Pump Components to Iran*** – On Feb. 5, 2009, two German nationals and a German company were indicted in the District of Massachusetts for conspiring to illegally export pump parts worth more than $200,000 to Iran in violation of the International Emergency Economic Powers Act. According to the indictment, Hans Schneider and Christof Schneider conspired with an individual in Jordan to obtain pump parts from a U.S. company for centrifugal sulphuric acid and sulphur pumps located in Iran. The pump parts would be delivered to Germany and re-exported to Iran by the defendants via their company, Schneider Gmbh. The case was investigated ICE and BIS.

- ***Stolen Military Optics Sold Overseas via Internet*** – On Feb. 2, 2009, brothers Timothy and Joseph Oldani pleaded guilty in the Southern District of West Virginia to charges of conspiring to steal military-grade optics from the U.S. Marine Corps and illegally export them overseas. Joseph Oldani admitted that while on active duty with the Marines, he stole military optics from his station in Kings Bay, Ga. Joseph admitted that he transported the stolen optics to his brother Timothy in Scott Depot, W.Va., where Timothy sold the stolen items on the Internet, primarily via eBay. The pair sold miniature night vision sights and target pointer illuminators via the Internet to purchasers in Hong Kong, Taiwan, and Japan. The investigation was conducted by DCIS and ICE.

- ***Restricted Nuclear Materials to Foreign Government*** – On Jan. 26, 2009, Roy Lynn Oakley, of Harriman, Tenn., pleaded guilty in the Eastern District of Tennessee to unlawful disclosure of restricted data under the Atomic Energy Act in connection with his efforts to sell materials used in the production of highly enriched uranium to a foreign government. Oakley had worked as a contract employee at the East Tennessee Technology Park (ETTP), in Oak Ridge, Tenn., which was previously a Department of Energy facility that produced highly enriched uranium. While employed at ETTP, Oakly stole restricted nuclear materials from the facility and offered them for sale to the French government. The French government officials did not pursue the purchase of these items. The FBI launched an undercover investigation posing as an agent of the foreign government and arrested Oakley after he offered them the nuclear materials in exchange for $200,000 cash. The materials involved were pieces of equipment known as "barrier" and associated hardware items that play a crucial role in the production of highly enriched uranium. The investigation was conducted by the FBI and Department of Energy.

- ***Restricted Electronic Components to China*** – On Jan. 20, 2009, Michael Ming Zhang and Policarpo Coronado Gamboa were arrested pursuant to indictments in the Central District of California charging them with separate schemes involving the illegal export of controlled U.S. electronic items to China and the illegal trafficking of counterfeit electronic components from China into the United States. Zhang was the president of J.J. Electronics, a Rancho Cucamonga, CA, business, while Gamboa owned and operated Sereton Technology, Inc., a Foothill Ranch, CA, business. Zhang allegedly exported to China dual-use electronic items that have uses in U.S. Army battle tanks. He also allegedly imported and sold in the United States roughly 4,300 Cisco electronic components bearing counterfeit marks from China. Gamboa is charged with conspiring with Zhang to import Sony electronic components with counterfeit marks from China for distribution in the United States. The case was investigated by the FBI, BIS, DCIS, ICE, the U.S. Postal Inspection Service, and the Orange County Sheriff's Department, in conjunction with the EAGLE Task Force in the Central District of California.

- ***Night Vision Technology to Singapore*** – On Jan. 15, 2009, Thomas J. Loretz was indicted in the District of Massachusetts for illegally exporting defense articles and making false statements in connection with the illegal export of sophisticated night vision technology to Singapore. Specifically, Loretz was charged with illegally exporting to Singapore hundreds of Imaging Grade Micro-Channel Plates and Premium Grade Micro-Channel Plates, which are used for military night vision optics. Loretz allegedly submitted false shipper's export documents to the government stating that the plates were commercial. The investigation was conducted by ICE.

- ***Restricted Integrated Circuits to China*** – On Jan. 12, 2009, William Chai-Wai Tsu, a resident of Beijing and the vice president of a Hacienda Heights, CA, company called Cheerway, Inc., made his initial court appearance in the Central District of California after being arrested on a criminal complaint charging him with illegally exporting national security controlled integrated circuits to China in violation of the International Emergency Economic Powers Act. According to the complaint, Tsu illegally exported to China at least 200 of the dual-use circuits, which have applications in sophisticated communications and military radar systems. Tsu allegedly purchased the items from a San Jose-based company after telling representatives of the company that he was not exporting the circuits. The investigation was conducted by agents from BIS and the FBI, with assistance from ICE and DCIS in connection with the EAGLE Task Force in the Central District of California.

- ***Thermal Imaging Cameras to China*** – On Dec. 31, 2008, Sam Ching Sheng Lee, Part-Owner and Chief Operations Manager of Multimillion Business Associate Corporation ("MBA"), and his nephew, Charles Yu Hsu Lee, made initial court appearances in the Central District of California on federal charges related to a conspiracy to procure and illegally export sensitive technology to China. Sam Lee, 63, native of China, and Charles Lee, 31, native of Taiwan, were arrested on Dec. 30, 2008 in Hacienda Heights, California. Both men are charged in an indictment filed on December 16, 2008, with felony counts of conspiracy and exporting national security controlled items without a license in violation of the International Emergency Economic Powers Act and Export Administration Regulations. The indictment alleges that the defendants, doing business as MBA, an import/export business located in Hacienda Heights, assisted persons in China to illegally procure export controlled thermal-imaging cameras. During the period between April 2002 and July 2007, defendants allegedly exported a total of ten thermal-imaging cameras to China in circumvention of export laws. After being advised of strict export restrictions, Charles Lee allegedly purchased the cameras from U.S. suppliers for approximately $9,500 a piece by withholding the fact that the devices were destined to China. His uncle, Sam Lee, then received the devices and through his company, arranged for their shipment to Shanghai, China without

obtaining proper licenses. One of the recipients is alleged to be an employee of a company in Shanghai engaged in the development of infrared technology. The thermal-imaging cameras are controlled for export to China by the Department of Commerce for national security and regional stability reasons because of their use in a wide variety of military and civilian applications. This investigation was conducted by the EAGLE Task Force in the Central District of California.

- ***Military Night Vision Systems to Vietnam*** -- On Dec. 16, 2008, federal authorities arrested Liem Duc Huynh pursuant to a December 3, 2008 indictment in the Central District of California charging him and two other defendants Dan Tran Dang and George Ngoc Bui with Arms Export Control Act violations. Dang is expected to make his initial court appearance in January 2009, while Bui remains a fugitive. According to the indictment, the defendants ran an export business called Professional Security, out of a Huntington Beach, California, residence, which illegally shipped at least 55 state-of-the-art night vision goggles to Vietnam in violation of the Arms Export Control Act. The three men are accused of conspiring to illegally ship Generation 3 Night Vision Goggles manufactured by ITT Industries to Vietnam. Because the goggles are classified as a "defense article" on the U.S. Munitions List, written permission must be obtained from the U.S. Department of State to legally export them. The charges against the men stem from an undercover investigation by ICE, the U.S. Naval Criminal Investigative Service (NCIS) and BIS.

- ***Software Stolen From Nuclear Plant to Iran*** – On Dec. 16, 2008, Mohammad Reza Alavi, a former employee of the Palo Verde Nuclear Generating Station in Arizona, was sentenced in the District of Arizona to 15 months in prison for illegally accessing a protected computer and for transportation of stolen software. On June 25, 2008, Alavi pleaded guilty to transporting stolen property in interstate commerce, in connection with his theft of software belonging to the Arizona nuclear plant that was valued at $400,000. On May 28, 2008 a jury also convicted Alavi of unauthorized access to a protected computer. Alavi served as a software engineer in the Simulator Support Group at the nuclear plant, which maintained a simulator system to train control room employees on the operation of nuclear reactors. The simulator system utilizes software to replicate current reactor status at Palo Verde allowing an operator to artificially create various incidents to train employees on safety and protocol procedures. The government presented evidence at trial that, after Alavi gave Palo Verde notice of his intent to terminate employment, he installed this software on his personal laptop without permission of Palo Verde. Alavi admitted that he took the software to Iran for use in future employment in the nuclear industry. Alavi's conduct was uncovered when he accessed the software vendor's website from Iran and obtained a code which allowed the software to be unlocked and activated. Alavi was indicted on April 12, 2007, following his arrest that month upon returning to the United States. The FBI conducted the investigation.

- ***Military Night Vision Equipment to Hizballah*** -- On Dec. 12, 2008, in the Eastern District of Michigan, Fawzi Assi was sentenced to ten years' imprisonment for attempting to provide material support to Hizballah, a foreign terrorist organization. Assi's offense conduct took place in 1998, when he attempted to board an airplane at Detroit Metro Airport with restricted military items destined for two men in Lebanon whom he believed to be members of Hizballah. Specifically he attempted to illegally export night vision goggles, global positioning satellite modules, and a thermal imaging camera. Assi pled guilty on Nov. 29, 2007. Assi had been a fugitive until he voluntarily surrendered to the FBI in Lebanon and was flown to the United States on May 17, 2004. The case was investigated by the FBI and ICE.

- ***Trade Secrets to China*** -- On Dec. 9, 2008, in the Northern District of Illinois, Hanjuan Jin was charged in a superseding indictment that added three counts of economic espionage in violation

of 18 U.S.C. § 1831. The charges were added to an April 1, 2008, indictment that charged Jin with theft of trade secrets under 18 U.S.C. § 1832. Jin is a former Motorola employee who started with the company in 1998. On February 28, 2007, one day after quitting Motorola, Jin was stopped at O'Hare airport with over 1,000 Motorola documents in her possession, both in hard copy and electronic format. A review of Motorola computer records showed that Jin accessed a large number of Motorola documents late at night. At the time she was stopped, Jin was traveling on a one-way ticket to China. The section 1831 charges are based on evidence that Jin intended that the trade secrets she stole from Motorola would benefit the Chinese military. Motorola had spent hundreds of millions of dollars on research and development for the proprietary data that Jin allegedly stole. The investigation was conducted by the FBI, with assistance from U.S Customs and Border Protection.

- ***Electronic Components to China*** – On Dec. 5, 2008, Zhen Zhou Wu, Yufeng Wei, and Bo Li were arrested and charged in the District of Massachusetts with conspiring to file, and causing others to file, false export documents in connection with U.S.-origin electronics exported to China. The defendants were officers and employees of Chitron Electronics Inc.,(Chitron-USA), a Massachusetts corporation that was wholly owned by Chitron Electronics Company, Ltd (Chitron-China), a company based in Shenzhen, China. The complaint alleges that Chitron-USA filed hundreds of false shipper's export declarations in an effort to circumvent U.S. export control laws. Wu was also charged with tax violations and making false statements. The investigation was conducted by BIS, ICE, FBI, and IRS.

- ***Stolen Trade Secrets to Chinese Nationals*** – On Nov. 21, 2008, Fei Ye and Ming Zhong were sentenced in the Northern District of California to one year in prison each, based in part on their cooperation, after pleading guilty on Dec. 14, 2006 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. They were first indicted on Dec. 4, 2002. The investigation was conducted by ICE, FBI and CBP.

- ***Lab Equipment & Computers to Iran*** – On Nov. 17, 2008, the U.S. Attorney for the Eastern District of Pennsylvania unsealed an indictment charging Mohammad Reza Vaghari and Mir Hossein Ghaemi with violations of the International Emergency Economic Powers Act for illegally exporting a variety of U.S.-origin goods to the United Arab Emirates for ultimate delivery to Iran. Operating through a Pennsylvania company called Saamen Company, the defendants allegedly illegally exported computers, fuel cell systems, ultrasonic liquid processors, ultrasound machines, and other laboratory equipment. The investigation was conducted by the FBI and BIS.

- ***Missiles, Grenade Launchers & Other Weapons to Sri Lankan Terrorists:*** On Oct. 30, 2008 in the District of Maryland, Haniffa Bin Osman was sentenced to 37 months in prison for conspiracy to provide material support to a designated foreign terrorist organization and money laundering. Haniffa Bin Osman conspired with several others to provide material support to the Tamil Tigers, a designated foreign terrorist organization and attempted to illegally export arms, including state of the art firearms, grenade launchers, night vision devices, surface to air missiles and unmanned aerial vehicles. According to the plea agreement, from April 2006, to September 29, 2006 Osman conspired with Haji Subandi, Erick Wotulo, and Thirunavukarasu Varatharasa, to provide state of the art firearms, machine guns, and ammunition, surface to air missiles, night vision goggles and other military weapons to the Liberation Tigers of Tamil Eelam (Tamil Tigers) operation within Sri Lanka, to be used to fight against Sri Lankan government forces. The conspirators contacted

an undercover business in Maryland about the sale of military weapons, requesting price quotes and negotiating the purchases. Subandi sent an itemized list of 53 military weapons, including sniper rifles, machine guns and grenade launchers that he wanted to acquire for the Tamil Tigers. Subandi advised the undercover business that Osman would inspect the weapons for the Tamil Tigers. Wotulo also advised that the chief of Tamil Tigers requested that he and Osman travel to Baltimore to meet with the undercover agents. On July 10, 2008, Wotulo, a retired Indonesian Marine Corps general, was sentenced to 30 months in prison for his role in the conspiracy. On Jan. 3, 2008, Varatharasa was sentenced to 57 months in prison. Subandi was sentenced to 37 months in prison on Dec. 14, 2007. Two additional defendants, Rinehard Rusli and Helmi Soedirdja, pleaded guilty to export and money laundering violations in January 2007 as part of a related plot to provide military night vision devices to the Indonesian military. The case was investigated by ICE, FBI, and DCIS.

- ***Stolen Military Night Vision Systems to Hong Kong*** – On Oct. 29, 2008, a criminal complaint was filed in the District of Hawaii against six U.S. Marines based at Kane'ohe Bay, Hawaii, for conspiring to illegally export stolen military night vision. Ryan Mathers, Charles Carper, Ronald William Abram, Jason Flegm, Mark Vaught, and Brendon Shultz were each charged with conspiracy to smuggle goods out of the United States. According to the complaint, the investigation began when agents learned that one of the defendants was selling stolen U.S. military night vision equipment on the Internet via eBay. A cooperating defendant subsequently purchased several night vision systems from the defendants, representing they would be illegally exported to Hong Kong. The case was investigated by ICE, DCIS, and NCIS.

- ***Violation of Trade Embargo with Iran*** – On Oct. 15, 2008, Seyed Mahmood Mousavi, a former interrogator for the Islamic Revolutionary Court in Iran, was sentenced in the Central District of California to 33 months in prison and a $12,500 fine for violating the trade embargo with Iran, false statements to the FBI, and filing a false tax return. Mousavi entered into consulting contracts to support a company in Iran in their efforts to bid for a mobile communication license and to establish a bank and leasing company in Iran. On April 24, 2008, Mousavi was convicted at trial of all counts of a June 8, 2007 indictment. The investigation was conducted by the FBI.

- ***Telecommunications Equipment to Iraq*** – On Oct. 2, 2008, Dawn Hanna was convicted by a jury in the Eastern District of Michigan on eight counts of an indictment charging her with illegally exporting telecommunications and other equipment with potential military applications to Iraq during the administration of Saddam Hussein and during the embargo on that country. Co-defendant Darrin Hanna was acquitted at trial. On July 19, 2007, both defendants were indicted on charges of conspiracy, violating the International Emergency Economic Powers Act, money laundering conspiracy, and false statements. From 2002 to 2003, the defendants allegedly received $9.5 million in proceeds to supply telecommunications and other equipment to Iraq in violation of the U.S. embargo that existed prior to the invasion by coalition forces in 2003. On March 25, 2009, Dawn Hanna was sentenced to six years in prison and ordered to pay $1.1 million, which represented profits to her and her business. This investigation was conducted by ICE, the Internal Revenue Service (IRS) and the FBI.

- ***Military Accelerometers to China*** – On Sept. 26, 2008, Qing Li was sentenced in the Southern District of California to 12 months and one day in custody, followed by three years of supervised released, and ordered to pay $7,500 for conspiracy to smuggle military-grade accelerometers from the United States to the People's Republic of China (PRC). Li pleaded guilty on June 9, 2008 to violating Title 18, USC Section 554. She was indicted for the offense on Oct. 18, 2007. According to court papers, Li conspired with an individual in China to locate and procure as

many as 30 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 g-forces of nuclear and chemical explosions. The investigation was conducted by ICE and the DCIS.

- ***Electronics & IED Components to Iran*** – On Sept. 18, 2008, a 13-count indictment was unsealed in the Southern District of Florida charging eight individuals and eight companies with conspiracy, violations of the International Emergency Economic Powers Act, the U.S. Iran embargo, and false statements in connection with their participation in conspiracies to illegally export electronics, Global Positioning Systems (GPS) systems, and other dual-use commodities to Iran. All the items had potential military applications, including in the construction of Improvised Explosive Devices (IEDs). Among other things, the indictment alleges the defendants illegally exported to Iran 345 GPS systems and 12,000 Microchip brand microcontrollers. These specific types of microcontrollers have been found in IEDs in Iraq. The businesses charged are: Mayrow General Trading, Atlinx Electronics, Micatic General Trading, Madjico Micro Electronics, and Al-Faris, all Dubai-based businesses; Neda Industrial Group, an Iran-based business; and Eco Biochem Sdn BHD and Vast Solution Sdn BHD, Malaysian businesses. The individuals charged are charged are: Ali Akbar Yahya and Farshid Gillardian, both Iranian nationals who are naturalized British citizens; F.N. Yaghmaei, Bahman Ghandi, Ahmad Rahzad, all Iranian nationals; Kaam Chee Mun, a resident of Malaysia; Djamshid Nezhad, a resident of Germany; and Majid Seif, an Iranian national residing in Malaysia. As part of the enforcement action, the Department of Commerce added 75 individuals and companies affiliated with this Iranian procurement network to its Entities list. This investigation was conducted by Commerce BIS, DCIS, ICE, and the Treasury Department's Office of Foreign Assets Control (OFAC.)

- ***Rifle Scopes to Russia*** – On Sept. 11, 2008, a grand jury in the Middle District of Pennsylvania indicted Boris Gavrilov, D&B Compas Ltd, and Kiflet Arm on charges of illegally exporting military-grade and dual-use rifle scopes to Russia without the required U.S. government licenses. Gavrilov is believed to be a resident of Israel. D&B Compas is located in Israel, while Kiflet Arm is located in Humboldt, Texas. Extradition proceedings for Gavrilov have commenced. The investigation was conducted by ICE and BIS.

- ***Controlled Technology to Indian Missile & Space Facility*** – On Sept. 9, 2008, in the District of Columbia, a grand jury returned a five-count indictment against Siddabasappa Suresh, an Indian national, and Rajaram Engineering Corporation, an Indian corporation, on charges of illegally supplying the Government of India with controlled goods and technology without the required licenses. According to the indictment, from 2001 to 2003, Suresh and Rajaram caused the illegal export of more than 100 controlled goods with an approximate value of $136,000. The indictment specifically identified six shipments to Vikram Sarabhai Space Centre (VSSC), which was within the Department of Space of the Government of India and responsible for research, development, and production of India's space launch system. These activities encompassed both civilian spacecraft and ballistic missiles. All of these transactions involved complex electronic instruments used in high performance testing and monitoring essential in the research and development of launching systems, including missile delivery systems. The investigation was conducted by the Department of Commerce BIS.

- ***Fighter Jet Components to Iran*** -- On Sept. 5, 2008, George Frank Myles, Jr. pleaded guilty to conspiring to illegally export military aviation parts without obtaining the permission of the State Department, in violation of the Arms Export Control Act. Myles was indicted for this offense on Sept. 6, 2007 in the Southern District of New York, and the case was transferred to the Southern

District of Florida pursuant to Rule 21. Sentencing is set for October 30, 2008. During the conspiracy, which spanned from April 2005 to March 2007, Myles supplied a number of military aviation parts, including F-14 parts, to an Iranian national, who allegedly picked up the parts in Dubai, United Arab Emirates and Bangkok, Thailand. This investigation was conducted by ICE.

- ***Ammunition to Mexico*** – On Sept 5, 2008, Noe Guadalupe Calvillo, Juan Luis Hernandez-Ramos, Guadalupe Ramiro Munoz-Mendez and Rogelio Garcia were sentenced to 46 months in prison, 37 months in prison, 30 months in prison, and 39 months in prison, respectively, after pleading guilty to illegally exporting thousands of rounds of ammunition to Mexico. Calvillo pleaded guilty to illegally exporting 51,400 rounds of ammunition, while Garcia, Hernandez-Ramos and Munoz-Mendez pleaded guilty to exporting 30,900 rounds of ammunition. The defendants were arrested and charged in Oct. 2007. This investigation was conducted by ICE.

- ***Military Technical Data on Unmanned Aerial Vehicles to China*** – On Sept. 3, 2008, J. Reece Roth, a former Professor Emeritus at the University of Tennessee, was convicted in the Eastern District of Tennessee of 15 counts of violating the Arms Export Control Act, one count of conspiracy, and one count of wire fraud. Roth had illegally exported military technical information relating to plasma technology designed to be deployed on the wings of Unmanned Aerial Vehicles (UAVs) or "drones" operating as a weapons or surveillance systems. The illegal exports involved technical data and information related to a U.S. Air Force research and development contract that Roth provided to foreign nationals from China and Iran. In addition, Roth carried multiple documents containing controlled military data with him on a trip to China and caused other controlled military data to be e-mailed to an individual in China. On Aug. 20, 2008, Atmospheric Glow Technologies, Inc (AGT), a privately-held plasma technology company in Tennessee, also pleaded guilty to charges of illegally exporting U.S. military data about drones to a citizen of China in violation of the Arms Export Control Act. Roth and AGT were first charged on May 20, 2008 in an 18-count indictment. In a related case, on April 15, 2008, Daniel Max Sherman, a physicist who formerly worked at AGT, pleaded guilty to an information charging him with conspiracy to violate the Arms Export Control Act in connection with this investigation. The investigation was conducted by the FBI, ICE, U.S. Air Force Office of Special Investigations, DCIS and BIS.

- ***Military Aircraft Components to China and Iran*** -- On Aug. 28, 2008, Desmond Dinesh Frank, a citizen and resident of Malaysia, was sentenced to 23 months in prison after pleading guilty on May 16, 2008, to several felonies in the District of Massachusetts in connection with a plot to illegally export military items to China and Iran. A six-count indictment returned on Nov. 15, 2007 charged Frank, the operator of Asian Sky Support, Sdn., Bhd., in Malaysia, with conspiring to illegally export items to Iran, conspiring to illegally export C-130 military aircraft training equipment to China, illegally exporting defense articles, smuggling, and two counts of money laundering. Frank was arrested in Hawaii on Oct. 8, 2007 by ICE agents. Frank conspired with others to illegally export and cause the re-export of goods, technology and services to Iran without first obtaining the required authorization from the Treasury Department. He also conspired with others to illegally export ten indicators, servo driven tachometers -- which are military training components used in C-130 military flight simulators -- from the United States to Malaysia and ultimately, to Hong Kong, China, without the required license from the State Department. This investigation was conducted by ICE, BIS, and DCIS.

- ***Forklift Parts to Iran*** – On Aug. 26, 2008, Robert E. Quinn pleaded guilty in the District of Colombia to a criminal information filed on July 9, 2008 alleging that he knowingly made false statements in connection with the illegal export of forklift parts to Iran. On Aug. 4, 2006, David

Tatum was sentenced to one year probation and a $5,000 fine, in connection with the illegal export of forklift parts to Iran by Clark Material Handling Corporation via Sharp Line Trading in Dubai, United Arab Emirates. On Jan. 19, 2006, Khalid Mamood, doing business as Sharp Line Trading, was sentenced to 17 months in prison. The case was investigated by ICE and BIS.

- ***Military Laser Aiming Devices & Fighter Pilot Cueing Systems to Taiwan*** – On Aug. 18, 2008, Yen Ching Peng was arraigned in Southern District of New York on Arms Export Control Act violations, as well as money laundering and smuggling violations after being extradited from Hong Kong. Among other things, Peng allegedly attempted to illegally export to Taiwan infrared laser aiming devices, thermal weapons sights, and a Joint Helmet Mounted Cueing System. On occasion, Peng requested that military items be delivered to his associate, Peter Liu, in New York for delivery in Taiwan. On Dec. 11, 2007, Peng was arrested in Hong Kong, while Liu was arrested in New York. Liu later pleaded guilty and was sentenced to 30 months in prison on Aug. 7, 2008. The investigation was conducted by ICE and DCIS.

- ***Missile Technology to Indian Government Entities*** -- On Aug. 11, 2008, in the District of Columbia, Mythili Gopal was sentenced to four years' probation and fined $5,000 after pleading guilty on Oct. 30, 2007 to one count of conspiracy to violate the International Emergency Economic Powers Act and the Arms Export Control Act. Gopal cooperated with the government against her co-conspirator, Parthasarathy Sudarshan, who on June 16, 2008, was sentenced to 35 months in prison. Sudarshan, the owner of an international electronics company called Cirrus Electronics, pleaded guilty in March 2008 to conspiring to illegally export 500 controlled microprocessors and other electronic components to government entities in India that participate in the development of ballistic missiles, space launch vehicles, and combat fighter jets. Among the recipients of the U.S. technology were the Vikram Sarabhai Space Centre and Bharat Dynamics, Ltd., two Indian entities involved in ballistic missile production, as well as the Aeronautical Development Establishment, which is developing India's Tejas fighter jet. Sudarshan was one of four defendants indicted in the case on March 8, 2007. Sudarshan and Gopal were arrested in South Carolina on March 23, 2007. The other two defendants, Akn Prasad and Sampath Sundar remain at large. Court documents in the case indicate Sudarshan was working with an Indian government official located in Washington, D.C. as part of the conspiracy. The investigation was conducted by the FBI, BIS, and ICE.

- ***Equipment to Iran*** – On Aug. 11, 2008, Nicholas D. Groos entered a guilty plea in the Northern District of Illinois to three counts of violating the International Emergency Economic Powers Act and one count of making false statements in connection with a scheme to transship U.S.-origin firefighting equipment to Iran using his position as director of a Viking Corporation subsidiary in Luxemburg. Groos was indicted on May 3, 2007. The case was investigated by ICE and BIS.

- ***Engineering Software to Iran*** – On Aug. 7, 2008, James Angehr and John Fowler, the owners of Engineering Dynamics, Inc. were sentenced to five years probation, fined $250,000 and ordered to forfeit $218, 583. On April 24, 2008, both pleaded guilty to a one-count information charging them with conspiring to violate the International Emergency Economic Powers Act in connection with a plot to export controlled engineering software to Iran. Engineering Dynamics, Inc, was a Louisiana company that produced software to design offshore oil and gas structures. As part of the case, on May 22, 2008, in the Eastern District of Louisiana, Nelson S. Galgoul, a resident of Brazil and the director of Suporte, a Brazilian engineering company, was sentenced to 13 months in prison for violating the International Emergency Economic Powers Act. Galgoul pleaded guilty on Aug. 2, 2007, to exporting and attempting to export controlled engineering software to Iran without the required U.S. authorization. Galgoul was charged in May 2007. He acted as an agent

for Engineering Dynamics, Inc. in the marketing and support of this software and trained users of the software in Iran. As part of the same case. The investigation was conducted by ICE, BIS and FBI.

- ***Night Vision Goggles to Pakistan, Italy, South Korea*** – On July 31, 2008, Rigel Optics, Inc., pleaded guilty in the Southern District of Iowa to one count of violating the Arms Export Control Act in connection with an illegal export of night vision goggles, while its President, Donald Wayne Hatch, pleaded guilty to one count of false statements in connection with the case. The defendants were indicted on June 24, 2008 for illegally exporting military night vision systems to Pakistan, Italy, and South Korea. The investigation was conducted by ICE and BIS

- ***Telecommunications Systems to Iran*** – On July 28, 2008, Allied Telesis Labs, Inc. was sentenced in the Eastern District of North Carolina to a $500,000 criminal fine and was placed on probation for two years. The company pleaded guilty on March 18, 2008, to conspiracy to violate the International Emergency Economic Powers Act as part of a scheme to land and execute a $95 million contract with the Iranian Information Technology Company to rebuild the telecommunications systems of 20 Iranian cities. The company was first charged via criminal information on Jan. 23, 2008. The investigation was conducted by BIS.

- ***Infrared Assault Rifle Scopes to Indonesia*** -- On July 28, 2008, in the Western District of Wisconsin, Doli Syarief Pulungan was sentenced to 48 months in prison followed by three years supervised release. On May 6, 2008, Pulungan, a citizen of Indonesia, was convicted of conspiracy to violate the Arms Export Control Act in connection with a plot to illegally export 100 Leupold Mark 4 CQ/T Riflescopes to Indonesia. Pulungan was first charged on Oct. 1, 2007. The tactical riflescopes have infrared capability and are designed to attach to M-16 and AR-15 assault rifles. The investigation was conducted by the FBI.

- ***Night Vision Firearm Sights to Japan*** – On July 28, 2008, Tomoaki Ilshiba, a U.S. Army Captain, pleaded guilty in the Western District of Washington to conspiracy to smuggle goods from the United States. In his plea agreement, Iishiba admitted that he illegally shipped firearms parts including holographic night vision firearms sights to contacts in Japan. In October and December 2006, Iishiba shipped sixty holographic sights to a contact in Japan and purposely mislabeled the customs form for the shipment because he knew he needed a license to ship the firearms parts to Japan. Iishiba was charged on July 16, 2008. This investigation was conducted by ICE, DCIS, and the Army Criminal Investigation Command.

- ***Combat Gun sights to Sweden and Canada*** – On July 24, 2008, Euro Optics Inc., was sentenced in the Middle District of Pennsylvania to a $10,000 corporate fine, $800 special assessment, and five years of corporate probation after pleading guilty on March 17, 2008 to illegally exporting advanced combat gun sights to Sweden and Canada without the required licenses. Euro Optics was charged via criminal information on Oct. 5, 2007. This investigation was conducted by ICE and Department of Commerce BIS.

- ***Cryogenic Pumps to Iran*** – On July 17, 2008, Cryostar SAS, formerly known as Cryostar France, a corporation headquartered in France, was sentenced in the District of Columbia to a criminal fine of $500,000 and corporate probation of two years. On April 11, 2008, the company pleaded guilty to conspiracy, illegal export, and attempted illegal export of cryogenic submersible pumps to Iran without a license. Cryostar specialized in the design and manufacturing of cryogenic equipment, such as pumps, that are used to transport and process natural gases at

extremely cold temperatures. The company was charged on March 24, 2008. The investigation was conducted by BIS.

- ***Military Aircraft Components to UAE, Thailand*** – On July 17, 2008, in the Central District of California, Air Shunt Instruments, Inc., was sentenced to pay a criminal fine of $250,000 and a special assessment of $400 for making false statements on Shipper's Export Declaration in claiming that a military gyroscope being sent overseas in 2003 did not require an export license, when in fact the item required such a license. Air Shunt, a Chatsworth, California company that buys and sells aircraft and aerospace components, was charged via criminal information and pleaded guilty on July 15, 2008. John Nakkashian, a Vice President for International Sales at Air Shunt, was responsible for obtaining the required licenses for such exports. During the investigation, Nakkashian fled the country and remains a fugitive today. On May 20, 2008, Nakkashian was indicted on four counts of violating the Arms Export Control Act. The indictment alleges he illegally exported components for the J85 engine, used on the F-5 fighter jet, and other military items to Dubai, United Arab Emirates, without first obtaining the required export license from the State Department. The indictment also alleges that he illegally exported a military gyroscope to Thailand. The investigation was conducted by DCIS and ICE.

- ***Computer Software to Cuba*** – On July 15, 2008, Platte River Associates, a Colorado company, was charged in U.S. District Court in Denver by Information for trading with the enemy. The president of Platte River Associates, Jay E. Leonard, was charged in separate Information on July 15, 2008, for unauthorized access of a protected computer. According to the Platte River Associates Information, on or about October 2000, the corporation allegedly provided specialized technical computer software and computer training, which was then used to create a model for the potential exploration and development of oil and gas within the territorial waters of Cuba, without first having obtained a license. This case was investigated by ICE. In the second case, Leonard allegedly used a wireless network connection at Houston International Airport to access a password protected computer website server located in Georgia, belonging to Zetaware Inc., a Texas Corporation. The Information charges that the unauthorized information obtained by the defendant was done by means of interstate commerce. This case was investigated by the FBI.

- ***Military Night Vision Systems to Lebanon*** – On July 9, 2008, Riad Skaff, a naturalized U.S. citizen from Lebanon and former ground services coordinator at O'Hare International Airport, was sentenced in the Northern District of Illinois to two years in prison for using his position at the airport to help smuggle $396,000 in cash and illegally export weapons scopes, military night vision goggles, and a cellular phone "jammer" to Lebanon. The case resulted from an undercover operation in which agents posed as individuals interested in smuggling money and military items to Lebanon utilizing contacts at O'Hare airport to bypass security. On Aug. 17, 2007, Skaff pleaded guilty to all nine counts of an indictment charging him with bulk cash smuggling; entering an aircraft and airport area in violation of applicable security requirements with the intent to commit a felony; exporting and attempted export of defense articles without first obtaining a required export license; and attempted international export of merchandise, articles, and objects contrary to U.S. law. Skaff was first arrested on Jan. 28, 2007. The investigation was conducted by ICE and DCIS.

- ***Illegal Export of F-5 and F-14 Fighter Jet Components*** – On June 19, 2008, in the Southern District of New York, Jilani Humayun, a Pakistani citizen and resident of Long Island, New York, pleaded guilty to conspiracy to illegally export arms and to commit money laundering. He faces a maximum sentence of 30 years and a $1 million fine. Humayun was arrested on July 19, 2007, and charged by information on December 19, 2007, with Conspiracy to Violate the Arms

Export Control Act and Smuggle Goods from the United States, and Conspiracy to Violate the International Emergency Economic Powers Act. According to his plea, Humayun illegally exported parts for F-5 and F-14 military fighter jets to Malaysia which prosecutors said may have eventually ended up in Iran. In the process of exporting these parts, he created airway bills that misrepresented the contents and value of his shipments. Such exports are of particular concern because F-14 components are widely sought by Iran, which is currently the only nation in the world that still flies the F-14 fighter jet. Humayun formed his own company, Vash International, Inc., in 2004, then, on eleven separate occasions between January 2004 and May 2006, exported to Malaysia F-5 and F-14 parts, as well as Chinook Helicopter parts. This investigation was conducted by ICE, BIS, FBI and DCIS.

- ***Firearms to Canada*** – On June 19, 2008, Ugur Yildiz was arrested and charged in a criminal complaint in the Northern District of Illinois with illegally exporting some 220 firearms from Chicago to Canada in 2006. The investigation was conducted by ICE and the ATF.

- ***U.S. Military Source Code and Trade Secrets to China*** – On June 18, 2008, Xiaodong Sheldon Meng was sentenced in the Northern District of California to 24 months in prison, three-years of supervised release, and a $10,000 fine for committing economic espionage and violating the Arms Export Control Act. Meng pleaded guilty in August 2007 to violating the Economic Espionage Act by misappropriating a trade secret used to simulate motion for military training and other purposes, with the intent to benefit China's Navy Research Center in Beijing. He also pleaded guilty to violating the Arms Export Control Act for illegally exporting military source code involving a program used for training military fighter pilots. Meng was the first defendant in the country to be convicted of exporting military source code pursuant to the Arms Export Control Act. He was also the first defendant to be sentenced under the Economic Espionage Act. Meng was charged in a superseding indictment on Dec. 13, 2006. The investigation was conducted by FBI and ICE.

- ***Valves to Iran*** – On June 9, 2008, CVC Services was sentenced in the Central District of California to a fine of $51,000 and five years probation for illegal transactions with Iran. In March 2008, the company pleaded guilty to selling to Iran valves that turn gas and oil pipelines on and off without a license. The company was charged on Jan. 31, 2008. The National Iranian Oil Company had sought the valves. This investigation was conducted by BIS.

- ***Controlled Amplifiers to China*** – On June 6, 2008, WaveLab, Inc. of Reston, Virginia, was sentenced in the Eastern District of Virginia to one year of supervised probation and a $15,000 fine, together with $85,000 in forfeiture previously ordered, for the unlawful export 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. WaveLab pleaded guilty on March 7, 2008 to a criminal information filed the same day. The investigation was conducted by BIS and ICE.

- ***Firearms Components to Sudan*** – On June 6, 2008, Khalid Abdelgadir Ahmed was sentenced in the Eastern District of Virginia to five months in prison after pleading guilty on March 13, 2008, to unlawfully attempting to export assault rifle components to the Sudan. Another defendant, Entisar Hagosman, was sentenced to time served and two years supervised probation on June 6, 2008 after pleading guilty on Mar. 13, 2008 to making false statements relating to her activity.

Both defendants were charged in a complaint on Jan. 30, 2008. The investigation was conducted by ICE and BIS.

- ***Arms Exports to Russia*** – On June 6, 2008, the United States Attorney for the Middle District of Pennsylvania announced that a superseding indictment was returned against Russian nationals, Sergey Korznikov of Moscow, Mark Komoroski of Nanticoke, Pa, and two companies, D&R Sports Center and Tactica Limited. The indictment charged them with conspiring to smuggle military equipment, including rifle scopes, magazines for firearms, face shields, and other military equipment from the United States to Russian to be resold to unknown persons. The case was investigated by ICE, IRS, ATF, U.S. Postal Service, Department of Commerce and DCIS.

- ***Theft of Military Trade Secrets to Sell to Foreign Governments*** -- On May 16, 2008, Allen W. Cotten of El Dorado Hills, California, was sentenced in the Eastern District of California to two years in prison for theft of trade secrets. Cotten pleaded guilty on Feb. 29, 2008, admitting that while employed at Genesis Microwave Inc., he stole items including plans, designs and parts for the manufacture and testing of detector logarithmic video amplifiers (DLVA) and successive detection logarithmic video amplifiers (SDLVA), which are components used in microwave technologies. These technologies have military applications that include enhancing navigational and guidance capabilities; radar jamming; electronic countermeasures; and location of enemy signals. Cotten sold and offered for sale these items to foreign governments and foreign military contractors. The total amount of actual or intended sales to these companies was $250,000. Cotten was charged by criminal information on Jan. 30, 2008. The investigation was conducted by the FBI and BIS.

- ***Controlled Computers to Iran*** – On May 15, 2008, Afshin Rezaei was sentenced in the Northern District of Georgia to six months' imprisonment and agreed to forfeit $50,000. Rezaei pleaded guilty on April 24, 2008 to one count of violating the International Emergency Economic Powers Act for the unlicensed export of computers to Iran via the United Arab Emirates. The computers were controlled for anti-terrorism reasons. Rezaei was indicted on Nov. 14, 2007. The investigation was conducted by BIS and ICE.

- ***Controlled Radiographic Equipment to Iran*** – On May 14, 2008, Bahram "Ben" Maghazehe pleaded guilty in the Southern District of New York to one count of false statements in connection with the illegal shipment of radiographic equipment to Iran. On August 14, 2007, Maghazehe was arrested pursuant to this shipment. Another individual, Jeff Weiss, pleaded guilty on Jan. 20, 2009 to a false statement charge in connection with his dealings with Maghazehe. The investigation was conducted by the FBI and BIS.

- ***Ammunition to Jamaica, Defense Training to UAE*** -- On May 12, 2008, Lance Brooks was charged in the Southern District of Florida with being an unlicensed broker of defense articles in connection with his efforts to broker the sale of 270,000 rounds of soft point ammunition to the Jamaica Constabulatory Force without the required license from the State Department. The case marked the second time Brooks had been charged with arms export violations. On Dec. 20, 2007, Brooks pleaded guilty to charges brought in Oct. 2007 that he exported defense training services on grenade launchers to the United Arab Emirates without a license. He was on bond pending sentencing in that case when the new charges against him were filed. The investigation was conducted by the FBI.

- ***Test Tube and Microplate Coating Systems to Iran*** – On May 1, 2008, Patrick Gaillard, the owner of Oyster Bay Pump Works, Inc., was sentenced in the Eastern District of New York after

pleading guilty to conspiracy to violate the International Emergency Economic Powers Act in connection with the planned export of restricted test tube and microplate coating systems to Iran through a trading company in the United Arab Emirates. The coating systems for microplates and test tubes produced by Oyster Bay are controlled for export and can be used in a wide variety of research and laboratory applications. On July 17, 2007, James Gribbon pleaded guilty to conspiracy to violate the Emergency Economic Powers Act in connection with the case. The investigation was conducted by BIS.

- ***Controlled Computer Equipment to Iran*** – On April 28, 2008, Mohammad Mayssami was sentenced in the Northern District of California to two years probation, a $10,000 fine and 160 hours of community service for his role in financing illegal exports to Iran. On Dec. 17, 2007, Mayssami pleaded guilty to failing to report a suspicious transaction for his part in financing export transactions by Super Micro Computer, Inc. He was originally charged by information on Dec. 3, 2007. Super Micro pleaded guilty on Sept. 18, 2006 to illegally exporting motherboards controlled for national security reasons to Iran and was sentenced to pay a criminal fine of $150,000., and agreed to pay an administrative fine of $125,400 to settle charges for related transactions. Super Micro was first charged on Sept. 1, 2006. The case was conducted by BIS.

- ***Military Night Vision Systems to Iran*** – On April 10, 2008, a British court ruled that Nosratollah Tajik should be extradited to the United States in connection with charges that he conspired to illegally export night vision weapons sights and military night vision goggles from the United States to Iran. Tajik plans to appeal the British High Court decision to the European Court of Human Rights. On Oct. 26, 2006, Tajik was arrested at his residence in County Durham in England by British law enforcement authorities, pursuant to U.S. charges filed in the Northern District of Illinois on Aug. 30, 2006. From December 1999 to October 2003, Tajik served as the Iranian Ambassador to Jordan. Tajik also held an honorary fellowship at England's University of Durham's Institute for Middle East and Islamic Studies. According to the August 2006 U.S. complaint, Tajik and a co-conspirator, Esmaiil Gharekhani, conspired to export to a variety of prohibited items from the United States to Iran via the United Kingdom, including night vision weapon sights and night vision goggles. The co-conspirator sent purchase orders to ICE agents for several controlled articles and asked that the goods be shipped from the U.S. to the United Arab Emirates for transshipment to Iran. During meetings in the United Kingdom, Tajik also allegedly asked agents about procuring a Swiss-manufactured 35mm naval gun capable of intercepting guided missiles. This investigation was conducted by ICE.

- ***Russian Attack Helicopters to Zimbabwe*** – On April 8, 2008, Peter Spitz, a resident of Hallandale, Fla., and the owner of Russian Aircraft Services LLC, was arrested in Miami pursuant to a criminal complaint alleging that he conspired to sell seven MI-24 Russian attack helicopters and three MI-8T Russian military transport helicopters to undercover law enforcement officials who represented that the helicopters would be going to a Cabinet member of the government of Zimbabwe. Spitz was charged in the Southern District of Florida with illegal arms brokering activities. The investigation was conducted by ICE and DCIS.

- ***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. On April 21, 2008, Chi Mak's brother, Tai Mak, was sentenced to 10 years imprisonment pursuant to a June 4, 2007, plea agreement in which he pleaded guilty to one count of conspiracy to export defense articles. On Oct. 2, 2008, Chi Mak's wife, Rebecca Chiu, was sentenced to 3 years in prison for her role in the plot. The investigation was conducted by FBI, NCIS, and ICE.

- ***Specialty Alloy Pipes to Iran*** – On March 14, 2008, Proclad International Pipelines, Ltd, a British corporation headquartered in Scotland, was sentenced in the District of Columbia to a criminal fine of $100,000 and corporate probation of five years for attempting to export from the United States to Iran via the United Kingdom and United Arab Emirates specialty alloy pipes without an export license from the U.S. government. Proclad pleaded guilty to one count of attempted export without an export license on Nov. 30, 2007 after being charged via information on Oct. 16, 2007. The investigation was conducted by ICE and BIS.

- ***Nuclear Testing Equipment to India*** – On March 12, 2008, MTS Systems Corp, of Eden Prairie, Minnesota, pleaded guilty in the District of Minnesota to two misdemeanor counts and was sentenced to two years probation and a $400,000 fine for submitting false export license applications to the Department of Commerce in connection with the proposed shipment of seismic testing equipment with nuclear applications to an entity in India. MTS knew the end-user in India would likely use the seismic testing equipment for nuclear purposes, but, in its export applications to the Department of Commerce, MTS falsely certified that the equipment would be used only for non-nuclear purposes. Commerce denied the export license. The company was charged on March 11, 2008. The investigation was conducted by BIS and ICE.

- ***100,000 Uzi Submachine Guns to Iran*** – On March 10, 2008, Seyed Maghloubi was sentenced to three years and five months in prison in the Central District of California to attempting to illegally export goods to Iran. As part of his Aug. 27, 2007, plea agreement, Maghloubi admitted that he had plotted to illegally export as many as 100,000 Uzi submachine guns as well as night vision goggles to officials in Iran's government. According to the facts of the plea agreement, the defendant sought to have the weapons shipped from the U.S. to Dubai and later transported over the border to Iran. Maghloubi was first charged on June 1, 2007. The investigation was conducted by the FBI and the Los Angeles Police Department.

- ***International Arms Dealer Charged with Conspiracy to Provide Weapons to Terrorists***: On March 6, 2008, a criminal complaint was unsealed in U.S. District Court for the Southern District of New York charging Viktor Bout, an international arms dealer, and his associate Andrew Smulian with conspiring to provide millions of dollars of weapons, including surface-to-air missiles and armor piercing rocket launchers, to the Fuerzas Armadas Revolucionarias de Colombia (FARC), a designated foreign terrorist organization based in Colombia. Bout was arrested on March 5, 2008 by Thai authorities in Bangkok, Thailand. According to the complaint, between November 2007 and February 2008, Bout and Smulian agreed to sell large quantities of weapons to two confidential sources working with the Drug Enforcement Administration (DEA) who held themselves out as FARC representatives acquiring these weapons for the FARC to use in Colombia. During one series of consensually recorded meetings in Romania, Smulian allegedly advised the confidential sources that Bout had 100 Surface-to-Air missiles available immediately; that Bout could also arrange to have a flight crew airdrop the weapons into Colombia using combat parachutes; and that Bout and Smulian would charge $5 million to transport the weapons. Bout engaged in multiple recorded phone calls with one of the DEA cooperating sources. The

United States plans to pursue the extradition of Bout from Thailand. Smulian has already made his initial court appearance in the Southern District of New York. This investigation was conducted by the DEA.

- ***Controlled Computers to Syria*** – On Feb. 14, 2008, Mazen Ghashim was sentenced in the Southern District of Texas to three years probation for violating the International Emergency Economic Powers Act and attempted export without a license. He was also ordered to forfeit computers and related equipment valued at $32,000. The violations occurred in February 2003 when Ghashim and his company KZ Results exported computers and related equipment to Syria without the required licenses. Ghashim was charged on Aug. 14, 2006, and pleaded guilty on Nov. 1, 2006. This investigation was conducted by BIS.

- ***Theft of Trade Secrets on U.S. Space Shuttle for China*** – On Feb. 11, 2008, Dongfan "Greg" Chung, a former Boeing engineer, was 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, 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 NASA.

- ***Two Sentenced in Iranian Embargo Case*** -- On Feb. 8, 2008, in the District of Columbia, Mojtada Maleki-Gomi was sentenced to 18-months and a $200,000 fine for violating the U.S. embargo against Iran for conspiring to sell textile machinery to Iran. Maleki-Gomi's son, Babak Maleki, was sentenced on the same day to probation for making false statements. On Sept. 29, 2006, Maleki-Gomi, his son, and a third defendant, Shahram Setudeh Nejad, were indicted for conspiracy to violate the International Emergency Economic Powers Act and the Iranian Transactions Regulations, and for violation of the United States Iranian Embargo. On November 19, 2007, Maleki-Gomi pled guilty to the conspiracy charge and his son Babar Maleki pled guilty to a superseding information charging him with making false statements.

- ***Military Night Vision Systems Overseas*** – On Jan. 22, 2008, Green Supply, Inc., was sentenced in the Eastern District of Missouri to two years probation, a $17,500 fine and an $800 special assessment after pleading guilty in Nov. 2007 to export control violations involving the illegal export of controlled night vision systems. The company was charged via information on Nov. 2, 2007. The investigation was conducted by ICE and BIS.

- ***Firearms to Canada*** – On Jan. 11, 2008, in the Southern District of Florida, defendants Gary Roach and Laron Frazer were convicted on international firearms trafficking charges. The

defendants were charged on July 26, 2007, for their role in a scheme in which they used straw purchasers to obtain handguns in Florida, Alabama, and Georgia. They then smuggled the guns to Canada in the door panels of rental cars. This case was investigated by the ATF and ICE.

- ***Military Amplifiers to China*** – On Dec. 19, 2007, Ding Zhengxing, Su Yang and Peter Zhu were indicted in the Western District of Texas for Arms Export Control Act violations in connection with an alleged plot 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 in January 2008 after they traveled to Saipan to take possession of the amplifiers. Peter Zhu, of Shanghai Meuro Electronics Company Ltd., in China, remains at large. The case was investigated by ICE.

- ***Petrochemical Valves to Iran and Iraq*** – On Dec. 17, 2007, Andrew Freyer was sentenced to 17 months in prison and ordered to pay a $10,000 criminal fine for his part in a conspiracy to export U.S.-origin valves to Iran via Australia. On Aug. 15, 2007, Freyer was convicted at trial of one count of aiding and abetting. On Oct. 15, 2007, Sharon Doe, Inside Sales Manager for Crane Pacific Valves in California, was sentenced to three years probation after pleading guilty in Jan. 18, 2007 for her role in the export of petrochemical valves to Iran and Iraq through Australia in order to avoid the Export Administration Regulations. Both Freyer and Doe was charged on Dec. 1, 2006. This investigation was conducted by BIS.

- ***Military Night Vision Goggles Illegally Exported Overseas*** – On Dec. 11, 2007, Jerri Stringer was sentenced to 48 months of imprisonment and three years of supervised release in the Northern District of Florida after pleading guilty to several violations in connection with a conspiracy with her son, former U.S. Air Force Staff Sgt. Leonard Allen Schenk, to steal restricted military night vision goggles, aviation helmets, and other equipment from the Air Force and sell them to overseas buyers. On Dec. 6, 2007, Schenk was sentenced to 235 months of imprisonment and three years of supervised release after pleading guilty to a 21-count indictment alleging the sale of stolen military equipment overseas and attempting to hire an undercover agent to kill a potential government witness. Schenk and Stringer were charged in the superseding indictment brought on Aug. 21, 2007. This investigation was conducted by ICE.

- ***Military Night Vision Technology to China*** – On Dec. 3, 2007, Philip Cheng was 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 pleaded guilty on Oct. 31, 2006, to brokering the illegal export of Panther-series infrared camera, a device which makes use of "night vision" technology. He was indicted on June. 3, 2004. The technology used in the device was controlled for national security reasons by the United States Department of State. The case was the result of a joint investigation by ICE, the FBI, the Department of Commerce, and the IRS.

- ***Fighter Jet Components to Germany*** – On Nov. 30, 2007, Murray Rinzler and his company World Electronics, Inc, were sentenced in the District of Connecticut to a criminal fine of $20,000 after pleading guilty on March 26, 2007 to charges that they conspired to violate the Arms Export Control Act by sending F-14 fighter jet components and other military items to Germany. Rinzler was also sentenced to two years probation. Both defendants were charged via information on March 26, 2007. This investigation was conducted by ICE, DCIS and BIS.

- ***F-14 Fighter Jet Components and Other Military Items to Iran*** – On Nov. 20, 2007, a grand jury in the Southern District of New York returned an indictment charging Yousef Boushvash

with violating the Arms Export Control Act, smuggling, conspiracy to commit money laundering and other violations in connection with his alleged acquisition of F-14 military fighter jet components and other military parts from the United States for export to Iran. The grand jury later returned two superseding indictments against Boushvash adding new offenses. According to the charges, Boushvash operated a company in Dubai, United Arab Emirates, called Glasgow International LLC which served as a hub for his illegal arms deals. Boushvash and his co-conspirators allegedly contacted numerous suppliers in the U.S. via e-mail and had them illegally export military components to the UAE, Thailand, and other locations, for ultimate transshipment to Iran. Boushvash had been arrested by Hong Kong authorities on Oct. 29, 2007 in Hong Kong pursuant to a provisional warrant issued by the Southern District of New York. The Justice Department commenced extradition proceedings to bring Boushvash to New York. On April 11, 2008, days before the extradition hearing was scheduled to begin in Hong Kong, authorities in Hong Kong terminated the proceeding and released Boushvash from custody. Boushvash currently is a fugitive from justice and has been placed on Interpol's list of wanted suspects. Three of Boushvash's U.S. suppliers have been convicted in related cases. Lawrence Davis and Gwendolyn Douglas and George Frank Myles Jr. have all pleaded guilty in the Southern District of New York. This investigation was conducted by ICE and DCIS.

- ***Hawk Missile Batteries to Iran*** – On Nov. 9, 2007, in the Western District of Texas, Robert Caldwell was sentenced to 20 months in prison and two years supervised release for attempting to illegally export to Iran specialized batteries for the Hawk Air Defense Missile system. Caldwell, along with co-defendants, Robert Gibson and Christopher Harold Tappin, were charged for their roles in the export plot on Feb. 2, 2007. Gibson later pleaded guilty and was sentenced to serve a two-year prison term. Tappin remains a fugitive. The case was investigated by ICE.

- ***U.S. Stealth Missile Data & Military Secrets to China*** – On Oct. 26, 2007, Noshir Gowadia was 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 U.S, as well as unlawfully possessing classified information, and laundering funds paid to him by the Chinese government for his illegal defense work. The original indictment against Gowadia was returned on Nov. 8, 2005. The investigation was conducted by the FBI, Air Force Office of Special Investigations, IRS, CBP, and ICE.

- ***Pipe Cutting Machines to Iran*** – On Oct. 24, 2007, Roger Unterberger, Muhammad Bhatti, and Go-Trans (North America) Inc., three defendants involved with the investigation of Go-Trans (North American) Inc., were sentenced in the Northern District of Illinois after pleading guilty on Aug. 20, 2007 to making false statements in connection with the attempted export of pipe cutting machines to Iran via Germany. All were charged by criminal information on Aug. 1, 2007. In addition, on July 31, 2007, Mohammed Meshkin was indicted on one count of violating the International Economic Emergency Powers Act in connection with the case. The investigation was conducted by BIS and ICE.

- ***Nickel Powder to Taiwan*** – On Oct. 11, 2007, Theresa Chang was sentenced to three years probation and to pay a $5,000 criminal fine. One June 21, 2007, Chang pleaded guilty to one count of making false statements related to the export of nickel powder controlled for nuclear proliferation reasons to Taiwan without an export license. The investigation was conducted by BIS.

- ***Tractor Parts to Iran*** – On Oct. 11, 2007, Saied Shahsavarani, President of Tak Components, Inc. was sentenced to three years probation and a $1,000 criminal fine after pleading guilty on June 14, 2007 to one count of aiding and abetting the operation of an unlicensed money transmitting business. Also, on Oct. 11, 2007 Tak Components was sentenced to one year probation and to forfeit $38,016. On June 14, 2007, Tak Components pleaded guilty to 16 counts of violating the International Emergency Economic Powers Act. Tak Components illegally exported a variety of equipment to Iran, falsely claiming they were destined for the United Arab Emirates. Both defendants were charged on June 6, 2007. This investigation was conducted by ICE and BIS.

- ***Illegal Exports of F-4 and F-14 Fighter Jet Components*** – On Oct. 5, 2007, Abraham Trujillo and David Wayne of Ogden, Utah, were charged in the District of Utah with attempting to illegally export components for F-4 and F-14 fighter jets using the Internet. According to the charges, the defendants attempted to illegally export military cable assemblies, wiring harnesses and other restricted components to Canada in 2006 and 2007. Such exports are of particular concern because F-14 components are widely sought by Iran, which is currently the only nation in the world that still flies the F-14 fighter jet. The investigation was conducted by ICE and DCIS.

- ***Products with Nuclear & Missile Applications to Pakistan*** – On Oct. 4, 2007, SparesGlobal, Inc., a Pittsburgh company, was sentenced to pay a $40,000 criminal fine in the Western District of Pennsylvania for conspiring to falsify documents and make false statements about a 2003 illegal export to the United Arab Emirates (UAE) that ultimately ended up in Pakistan. According to court documents, SparesGlobal exported to a trading company in the UAE restricted graphite products that can be used in nuclear reactors and in the nose cones of ballistic missiles. The graphite products were routed to Pakistan. After the shipment, the company attempted to mislead federal investigators when questioned about the shipment and related documents. On July 7, 2007, SparesGlobal, represented by its President, Om Sharma, pleaded guilty. The company was charged via information on April 23, 2007. The investigation was conducted by BIS.

- ***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. The case was investigated by the FBI.

- ***Sensitive Aircraft Components to Iran*** – On Sept. 18, 2007, Aviation Services International, a Netherlands-based aviation services company, its owner, Robert Kraaipoel, and two other Dutch companies, Delta Logistics and TPC, were charged in the District of Columbia with illegally exporting aerospace grade aluminum, aircraft components, and other equipment to Iran and the government of Iran. The complaint alleges that, in 2006 alone, Aviation Services obtained some 290 aircraft-related components from the U.S. and caused them to be shipped to Iran. Many of

these U.S.-origin goods were sent to Iranian government agencies, Iranian procurement agencies or companies doing business in Iran, according to the complaint. The investigation was conducted by BIS, ICE, DCIS and FBI.

- ***Restricted Technology to China*** – On Aug. 1, 2007, Fung Yang, the president of Excellence Engineering Electronics, Inc., pleaded 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. Yang was charged by information on July 31, 2007. The investigation was conducted by BIS and the FBI.

- ***Radios, Ammunition Magazines, Scopes to Designated Terrorist in Philippines*** – On Aug. 1, 2007, Rahmat Abdhir was indicted in the Northern District of California on charges of conspiracy to provide material support to terrorists, providing material support to terrorists, and contributing goods and services to a Specially Designated Global Terrorist. According to the indictment, Rahmat Abdhir communicated frequently with Zulkifli Abdhir, his fugitive brother and a U.S.-specially designated terrorist who operates in the Philippines and is a member of the central command of *Jemaah Islamiyah*. From his home in California, Rahmat allegedly sent his brother money, two-way radios, Colt .45 magazines, binoculars, rifle scopes, batteries and other materials, even as his brother evaded capture and battled Philippine troops. Zulkifli Abdhir was charged in the same indictment with conspiracy to provide material support to terrorists and providing material support to terrorists. The investigation was conducted by the FBI and ICE.

- ***Aircraft Components to Iran*** – On July 30, 2007, Ali Khan, the owner of TurboAnalysis in Phoenix, AZ, was sentenced in the Eastern District of New York to five years probation, a $1.4 million forfeiture, and $100,000 criminal fine in connection with his role in a conspiracy to illegally export aircraft components to Iran. Khan previously pleaded guilty to one count of conspiracy to violate the International Emergency Economic Powers Act in Sept. 2005. He was indicted on May 5, 2004. This investigation was conducted by BIS and ICE.

- ***Sensitive Technology to Prohibited Facility in India*** – July 30, 2007, Samuel Shangteh Peng was charged in the Central District of California with illegally exporting sensitive technology to an entity in India prohibited from receiving such technology due to proliferation concerns. Peng, an international sales manager at a California company, was charged with illegally exporting vibration amplifiers, cable assemblies and vibration processor units in 1999 and 2000 from the U.S. to Hindustan Aeronautics Limited, Engine Division, in India. In 1998, the U.S. government designated this facility in India as an end-user of concern for proliferation reasons. The investigation was conducted by BIS, ICE, and the Naval Criminal Investigative Service (NCIS).

- ***Missiles, Explosives, Arms to Overthrow Government in Laos*** – On June 14, 2007, a grand jury in the Eastern District of California returned an indictment charging 11 defendants with conspiring to overthrow the government of Laos by force and violence. Among other things, the defendants were charged with conspiring to acquire hundreds of assault rifles, Stinger missiles, anti-tank missiles, mines, and C-4 explosives which they intended to ship to safe houses in Thailand and Laos for use in overthrowing the government of Laos. Harrison Ulrich Jack, Vang Pao, Lo Cha Thao, Lo Thao, Yua True Vang, Hue Vang, Chong Yang Thao, Seng Vue, Chue Lo, Nhia Kao Vang, and Dang Vang were charged in the indictment with conspiracy to violate the Arms Export Control Act, conspiracy to violate the Neutrality Act, conspiracy to kill, kidnap, and maim; conspiracy to possess a missile system to destroy aircraft, and other violations. The investigation was conducted by the ATF and FBI.

- ***F-14 Fighter Jet Components to Iran*** – On May 8, 2007, Reza Tabib was sentenced in the Central District of California to violating the International Emergency Economic Powers Act in connection with his efforts to illegally export military aircraft parts to Iran via associates in Germany and the United Arab Emirates. In 2006, federal agents intercepted maintenance kits for the F-14 fighter jet that Tabib and his wife, Terri Tabib, had sent to Iran. A search of their California home led to the seizure of more than 13,000 aircraft parts as well as various aircraft part "shopping lists" that provided to the couple by an Iranian military officer. Reza Tabib pleaded guilty on June 5, 2006 after being charged in Feb. 2006. His wife Terri pleaded guilty on Dec. 14, 2006. The investigation was conducted by ICE and DCIS.

- ***Controlled Telecommunications Equipment to Cuba*** – On April 25, 2007, LogicaCMG Inc., pleaded guilty in the District of New Hampshire and was sentenced to pay a $50,000 criminal fine for illegally causing goods to be exported to Cuba. In 2001, LogicaCMG's predecessor company, CMG Telecommunications, exported telecommunications equipment controlled for national security reasons to Cuba via Panama without the required export license. The company was charged by information on March 30, 2007. This case was investigated by ICE and BIS.

- ***Military Night Vision Components to India*** – On April 19, 2007, a jury in the Western District of Pennsylvania convicted Electro-Glass Products, a Pennsylvania company, of violating the Arms Export Control Act. Evidence at trial established that Electro-Glass illegally exported 23,000 solder glass performs, which are components of military night vision equipment, to a company in India without the required State Department license. The company was indicted on April 5, 2006. The investigation was conducted by ICE.

- ***Telecommunications Equipment from China to Iraq*** – On April 10, 2007, Andrew Huang, the owner of McAndrew's, Inc, an international export company, pleaded 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. The investigation was conducted by the FBI, ICE, NCIS, IRS and BIS.

- ***Ballistic Helmets to Suriname*** – On March 28, 2007, Alpine Armoring, Inc., a Virginia company, pleaded guilty in the Eastern District of Virginia to the unlicensed export of controlled ballistic helmets to Suriname. Fred Khoroushi, the president and director of Alpine Armoring, also pleaded guilty to making false statements on an export declaration. Both Alpine Armoring and Khoroushi were charged via information on March 27, 2007. The investigation was conducted by BIS, ICE, and DCIS.

- ***$100 Million Penalty for Illegal Exports of Military Night Vision Technology to China, Singapore, U.K.*** -- On March 27, 2007, ITT Corporation, the leading manufacturer of military night vision equipment for the U.S. Armed Forces, agreed to pay a $100 million penalty and admitted to illegally exporting restricted night vision data to China, Singapore, and the United Kingdom in the Western District of Virginia. The company also pleaded 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 of the most advanced night vision systems in the world for the U.S. Armed Forces. The investigation was conducted by DCIS and ICE.

- ***Machine Guns, Arms to Indonesia*** – On Jan. 18, 2007, Hadianto Djuliarso pleaded guilty in the Eastern District of Michigan to conspiracy to violate the Arms Export Control Act and money laundering in a scheme to purchase and illegally export more than $1 million worth of machine guns, sniper rifles and other weapons to Indonesia. According to court documents, Djuliarso also made inquiries about purchasing Sidewinder missiles and strafing ammunition for illegal export to Indonesia. Three other defendants, Ibrahim Bin Amran, Ignatius Soeharli, and David Beecroft, have pleaded guilty in this case. The investigation was conducted by ICE and DCIS.

- ***U.S. Anti-Submarine Torpedo Technology to South Korea*** – On Dec. 21, 2006, Stuart Choi pleaded guilty to an export violation for his role in a scheme to illegally export U.S. anti-submarine torpedo technology to South Korea. The technology was destined for the South Korean "Blue Shark" anti-submarine torpedo program made public during the summer of 2006. This investigation was conducted by ICE.

- ***Sensitive Technology to Iranian National*** – On Dec. 5, 2006, Seyed Rohani Eftekhari pleaded guilty in the Western District of Texas to attempting to purchase a "guided wave" scanning device with the intent of providing the unit to a third party from Iran without the required U.S. government license. He was charged on Oct. 4, 2006. The investigation was conducted by ICE and the FBI.

- ***Technology with Nuclear Applications to Iran*** – On Nov. 30, 2006, Juan Sevilla, sales director of United Calibration Corporation in California, was sentenced in the Northern District of Illinois for attempting to illegally export to Iran machinery and software to measure the tensile strength of steel in violation of the U.S. embargo. The technology is on the Nuclear Supplier's Group "Watch List" as a commodity that can make a contribution to nuclear activities of concern. Sevilla was indicted on March 1, 2005 and pleaded guilty on Sept. 14, 2005. The investigation was conducted by BIS and ICE.

- ***Rifle Scopes, Weapons to Iran*** – On Nov. 22, 2006, Fereidoon Kariman was arrested in the Eastern District of Michigan after authorities found rifle scopes, laser range finding binoculars, stun guns and other prohibited items in luggage for his trip to Iran. He pleaded guilty on Nov. 15, 2007 and was later sentenced on March 18, 2008. The investigation was conducted by ICE.

- ***Missile Technology / Military Accelerometers to Iran*** – On Nov. 13, 2006, officials with the Royal Thai Police arrested Jamshid Ghassemi in Bangkok, Thailand, pursuant to a provisional U.S. arrest warrant. Ghassemi and a co-conspirator, Aurel Fratila, had been indicted on October 17, 2006 in the Southern District of California on charges of conspiracy to violate the Arms Export Control Act, conspiracy to launder money, and money laundering. According to the indictment, the defendants attempted to illegally export military gyroscopes and military accelerometers suitable for ballistic missile guidance, as well as spacecraft navigation and control systems, to Romania for ultimate transshipment to Iran. Ghassemi was released by Thai authorities in Sept. 2008 after the U.S. extradition request was denied. He remains a fugitive. This investigation was conducted by ICE and DCIS.

- ***Military Weapons Scopes to China*** – On Oct. 25, 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. He pleaded guilty on Dec. 11, 2006. The investigation was conducted by DCIS, BIS, and ICE.

- ***U.S. Military Vehicles to the Middle East*** – On Oct. 24, 2006, Ronald Wiseman, a former Defense Reutilization and Marketing Service (DRMS) official, was sentenced in the District of Columbia for illegally selling militarized vehicles to individuals in Middle East nations. A second former DRMS official, Gayden Woodson, pleaded guilty the same day in connection with the scheme. Both were charged on May 5, 2005. The case was investigated by ICE, DCIS and the Defense Logistics Agency.

- ***Terrorist Transactions, Computer Exports to Libya and Syria*** – On Oct. 13, 2006, sentences were handed down in the Northern District of Texas against Infocom Corporation and Bayan Elashi, Ghassan Elashi and Basman Elashi in connection with prior convictions at trial for dealing in the funds of a Specially Designated Terrorist, a high-ranking official of the terrorist organization, Hamas, and conspiracy to export computers and computer equipment to Libya and Syria. The investigation was conducted by FBI, BIS, ICE, IRS and members of the North Texas Joint Terrorism Task Force.

- ***Aircraft Parts to Iran*** – On Oct. 13, 2006, Ernest Koh, doing business as Chong Tek, was sentenced in the Eastern District of New York to jail after his conviction at trial for obtaining components that can be used in C-130 military transport planes and P-3 Naval aircraft, and diverting those parts to Malaysia for ultimate transshipment to Iran. In total, the government found that Koh illegally exported roughly $2.6 million in aircraft parts to Iran. Koh was first charged on Oct. 26, 2005. The investigation was conducted by BIS and ICE.

- ***Industrial Furnace to Missile Institute in China*** – On Oct. 4, 2006, William Kovacs, the owner and president of Elatec Technology Corporation in Massachusetts, was sentenced in the District of Columbia to 12 months 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. Kovacs and Elatec pleaded guilty to conspiring to violate export laws on May 28, 2004. They were first charged on Nov. 13, 2003. An associate, Stephen Midgley, separately pleaded guilty on Jan. 10, 2005, to making false statements in export documents. The investigation was conducted by BIS and ICE.

###

08-959

RELEASE

Department of Justice

FOR IMMEDIATE RELEASE
TUESDAY, OCTOBER 28, 2008
WWW.USDOJ.GOV

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

MORE THAN 145 DEFENDANTS CHARGED IN NATIONAL EXPORT ENFORCEMENT INITIATIVE DURING PAST FISCAL YEAR

Three Charged Today in Plot to Export Sensitive Technology to China Space Entity

New Counter-Proliferation Task Forces & Training Part of National Effort

WASHINGTON -- A multi-agency initiative to combat illegal exports of restricted military and dual-use technology from the United States has resulted in criminal charges against more than 145 defendants in the past fiscal year, with roughly 43 percent of these cases involving munitions or other restricted technology bound for Iran or China, the Justice Department and several partner agencies announced today.

Over the past fiscal year, the National Export Enforcement Initiative has also resulted in the creation of Counter-Proliferation Task Forces in various judicial districts around the country. Today, there are approximately 15 such task forces or versions of them nationwide. In addition, the initiative has resulted in enhanced training for more than 500 agents and prosecutors involved in export control and the creation of new mechanisms to enhance counter-proliferation coordination among law enforcement agencies, export licensing agencies and the Intelligence Community.

Among the most recent cases brought in connection with the initiative was an indictment returned today in the District of Minnesota charging three individuals, Jian Wei Ding, Kok Tong Lim, and Ping Cheng, with conspiring to illegally export to the People's Republic of China (PRC) controlled carbon-fiber material with applications in rockets, satellites, spacecraft, and uranium enrichment process. According to the indictment, the intended destination for some of the material was the China Academy of Space Technology, which oversees research institutes working on spacecraft systems for the PRC.

Unveiled in Oct. 2007, the National Export Enforcement Initiative is a cooperative effort by the Justice Department's National Security Division (NSD), the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE), the Federal Bureau of Investigation (FBI), the Department of Commerce's Bureau of Industry and Security (BIS), the Pentagon's Defense Criminal Investigative Service (DCIS), the State Department's Directorate of Defense Trade Controls, the Treasury Department's Office of Foreign Assets Control and other agencies.

The Threat from Illegal Exports

On a daily basis, foreign states as well as criminal and terrorist groups seek arms, technology, and other materials to advance their technological capacity, weapons systems and, in some cases, Weapons of Mass Destruction programs. With America producing the most advanced technology in the world, it has become a primary target of these illicit technology acquisition efforts. The U.S. government, defense sector, private companies, and research institutions are routinely targeted as sources of these materials.

The items sought from America in these illicit schemes are as diverse as missile technology, nuclear technology, assault weapons, trade secrets, source code, military aircraft parts, night vision systems, and technical know-how. The improper transfer of these items poses threats to U.S. allies, U.S. troops overseas, and to Americans at home. It also undermines America's strategic, economic, and military position in the world.

"Keeping U.S. weapons technology and other restricted materials from falling into the wrong hands and from being used against our allies, our troops overseas or Americans at home is a top counter-intelligence priority of the Justice Department," said Patrick Rowan, Assistant Attorney General for National Security. "Through this multi-agency initiative we are making America a far more hostile target for those that seek to obtain our sensitive technology through illegal means."

Enhanced Prosecutions and Investigations

In recent years, as investigative agencies have stepped up their efforts to address this threat, the Justice Department has handled a growing number of cases involving illegal exports of sensitive U.S. technology and embargo violations. Last year, the Department decided to institutionalize the expansion of its export control efforts through the launch of the National Export Enforcement Initiative, which is designed to increase training and coordination among agencies involved in export control, enhance prosecution of these crimes, and deter illicit activity.

To implement the initiative, the Justice Department appointed its first National Export Control Coordinator in June 2007. In October 2007, the Department joined forces with counterparts from ICE, FBI, BIS, DCIS, the Department of State and other agencies to publicly announce the initiative. Since that time, the number of prosecutions has continued to grow, as investigative agencies have increased the tempo of their operations and prosecutors have become more familiar with this area of law.

During Fiscal Year (FY) 2008, there were more than 145 defendants charged in export control or embargo cases, compared to roughly 110 charged in FY 2007. There have been more than 255 defendants charged in such cases over the past two fiscal years. Charges brought in these cases include violations of the Arms Export Control Act, the International Emergency Economic Powers Act (IEEPA), the export control provision of the PATRIOT Reauthorization Act, the Trading with the Enemy Act, and other statutes.

Restricted Materials Bound for Iran and China

Roughly 43 percent of the defendants charged in FY 2008 were charged in export control or embargo cases involving Iran or China. In total, Iran ranked as the leading destination for illegal exports of restricted U.S. technology in the prosecutions brought in FY 2008, as well as those in FY 2007.

The illegal exports bound for Iran have involved such items as missile guidance systems, Improvised Explosive Device (IED) components, military aircraft parts, night vision systems and other materials. The illegal exports to China have involved rocket launch data, Space Shuttle technology, missile technology, naval warship data, Unmanned Aerial Vehicle or "drone" technology, thermal imaging systems, military night vision systems and other materials.

A significant portion of the cases in FY 2008 and in FY 2007 also involved illegal exports to Mexico. These prosecutions primarily involved illegal exports of firearms, including assault weapons and rifles, as well as large quantities of ammunition destined for Mexico. In addition, there were several cases during this period involving arms and other materials being routed to terrorist organizations in various nations.

New Counter-Proliferation Task Forces

The cornerstone of the initiative has been the ongoing formation of multi-agency Counter-Proliferation Task Forces in U.S. Attorney's offices around the country. Today, there are approximately 15 such task forces or working groups operating nationwide, some straddling more than one judicial district.

These entities have built on prior inter-agency efforts used in certain districts where agents from ICE, FBI, BIS, and Defense Department agencies pool data and jointly pursue cases. Under the leadership of U.S. Attorneys, these task forces foster coordination critical to the success of export control.

Enhanced Training and Coordination

Because export control cases involve complex statutory and regulatory schemes, sophisticated technology, international issues, agencies with different authorities, and, often classified information, training for prosecutors and agents has been a critical focus of the initiative.

Since January 2008 alone, the Justice Department's National Security Division has presented more than 30 legal training sessions and lectures around the country on export control. In addition, the Department has held two national export control training conferences and is scheduled to hold another in early 2009 in South Carolina. To date, more than 500 prosecutors and investigators have received training through these mechanisms.

The Department's National Security Division has also distributed a comprehensive tool kit of legal pleadings and related information on export control for field prosecutors and agents. On a daily basis, the National Export Control Coordinator provides legal advice and counsel for prosecutors and agents on these cases.

Another critical component of the initiative involves enhanced coordination within the export control community. The Justice Department, along with other agencies, has created the Technology Protection Enforcement Group (TPEG), an inter-agency Headquarters-level working group, to enhance export control coordination among law enforcement agencies and between law enforcement agencies and the Intelligence Community. In addition, the Department has created a working group of intelligence analysts to assist field prosecutors across the country in export cases and to ensure appropriate information sharing with the Intelligence Community.

The Department has also initiated monthly coordination meetings with the export licensing agencies, particularly the State Department's Directorate of Defense Trade Controls and the Commerce Department's BIS, to improve coordination and the flow of information to those agencies in accomplishing their missions. Furthermore, the Department regularly participates in and contributes to outreach efforts with foreign governments on export control matters, in conjunction with the State Department.

New Legislation

Over the past year, the Department has also been involved in a variety of legislative, regulatory, and policy proposals related to export control and embargos. During 2007, for instance, Congress passed and the President signed into law amendments to the International Emergency Economic Powers Act (IEEPA), which, among other things, added conspiracy and attempt provisions to the IEEPA as well as enhanced criminal fines and administrative fines for violations of this law, which is a critical export and embargo enforcement statute.

"We will not allow the United States' national security to be held hostage by rogue nations or sold to the highest bidder. This includes sensitive military information and technology, as well as weapons of mass destruction or the components needed to produce them. ICE is committed to working closely and cooperatively with our partners at every level of law enforcement to ensure this does not happen." Julie L. Myers, Assistant Secretary of Homeland Security for ICE said. "Time after time, our export enforcement investigations have helped prevent the illegal acquisition of these resources and helped maintain military, political and economic stability throughout the world."

"No one agency can accomplish the immense task of safeguarding U.S. national security assets and protecting the illegal export of restricted materials, including military and dual-use technologies," said Executive Assistant Director Arthur M. Cummings, II, of the FBI's National Security Branch. "The FBI is committed to enforcing export control laws and will continue to work closely with our partners in the law enforcement

and the intelligence communities to enhance export control awareness and training and to build on the success of our Counter-Proliferation Task Forces."

"We are continuing to sharpen our enforcement efforts to focus on those areas of greatest concern to us: proliferators, supporters of terrorism, and nations of illicit trans-shipment concern. When foreign companies take controlled U.S. technology and illegally transfer it - they also face serious repercussions. We remain committed to investigate, uncover, and stop these activities wherever they may occur," said Under Secretary of Commerce Mario Mancuso.

"Preventing the illegal export of critical technologies and restricted munitions is of extreme concern to the Department of Defense because of the real possibility that our Soldiers, Sailors, Airmen, and Marines may have to face this materiel in the hands of our adversaries and thereby lose the advantage that U.S. technology is supposed to provide them," said Charles W. Beardall, Department of Defense Deputy Inspector General for Investigations. "Protecting America's Warfighters through technology protection is a top priority for the Defense Criminal Investigative Service, the law enforcement arm of the DoD Inspector General, and a fundamental focus for our special agents."

"We applaud the Department of Justice's efforts," said John Rood, Acting Undersecretary of State for Arms Control and International Security. "We are pleased that the Department of State has been able to support this important initiative and proud of the tremendous success achieved so far in disrupting the flow of sensitive technology to our adversaries and protecting our national security and foreign policy interests."

Foreign Efforts to Obtain Controlled U.S. Technology

The technology at the heart of this initiative includes restricted U.S. military items, dual-use equipment, and other technical expertise or know-how, some of which have applications in Weapons of Mass Destruction. These materials are generally restricted and may not be exported without U.S. government approval. Foreign procurement networks intent on obtaining such materials from the U.S. rarely target complete weapons systems, but often focus on seemingly innocuous components to develop their own weapons systems.

According to recent reports by the Intelligence Community, private-sector businessmen, scientists, students, and academics from overseas are among the most active collectors of sensitive U.S. technology. Most did not initially come to the U.S. with that intent, nor were they directed to do so by foreign governments. Instead, after finding that they had access to technology in demand overseas, they engaged in illegal collection to satisfy a desire for profits, acclaim, or patriotism to their home nations.

At the same time, foreign government organizations remain aggressive in illegally acquiring sensitive U.S. technology. Some governments have established quasi-official organizations in the U.S. to facilitate contact with overseas scientists, engineers and businessmen. Foreign governments have been observed directly targeting U.S. firms;

employing commercial firms in the U.S. and third countries to acquire U.S. technology; and recruiting students, professors, and scientists to engage in technology collection.

# # #

08-958

RELEASE

Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, OCTOBER 11, 2007
WWW.USDOJ.GOV

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

JUSTICE DEPARTMENT AND PARTNER AGENCIES LAUNCH NATIONAL COUNTER-PROLIFERATION INITIATIVE

WASHINGTON, D.C. — The Justice Department and several partner agencies today launched a national initiative that will harness the counter-proliferation assets of U.S. law enforcement, licensing, and intelligence agencies to combat the growing national security threat posed by illegal exports of restricted U.S. military and dual-use technology to foreign nations and terrorist organizations.

The export enforcement initiative was announced by Kenneth L. Wainstein, Assistant Attorney General for National Security; Julie L. Myers, Homeland Security Assistant Secretary for U.S. Immigration and Customs Enforcement (ICE); Timothy D. Bereznay, Assistant Director, FBI Counterintelligence Division; Darryl W. Jackson, Assistant Secretary of Commerce for Export Enforcement; Charles W. Beardall, Director of the Defense Criminal Investigative Service (DCIS); and Stephen D. Mull, Acting Assistant Secretary of State for Political Military Affairs.

The threat posed by illegal foreign acquisition of restricted U.S. technology is substantial and growing. In the past week, there have been federal cases involving the illegal export of items with nuclear and missile applications to Pakistan and the illegal export of U.S. fighter jet components sought by Iran. A 2006 Defense Department report noted a 43 percent increase in the number of suspicious foreign contacts with U.S. defense firms, and an Intelligence Community report issued last year asserted that entities from a record 108 nations were engaged in efforts to obtain controlled U.S. technology.

China and Iran pose particular U.S. export control concerns. The majority of U.S. criminal export prosecutions in recent years have involved restricted U.S. technology bound for these nations as opposed to others. Recent prosecutions have highlighted illegal exports of stealth missile technology, military aircraft components, Naval warship data, night vision equipment, and other restricted technology destined for China or Iran.

"Foreign states and terrorist organizations are actively seeking to acquire U.S. data, technological knowledge and equipment that will advance their military capacity, their weapons systems and even their weapons of mass destruction programs. Many have targeted our government, industries and universities as sources of these materials," said Assistant Attorney General Wainstein. "This initiative is a coordinated campaign to keep

sensitive U.S. technology from falling into the wrong hands and from being used against our allies, against our troops overseas or against Americans at home."

New Counter-Proliferation Task Forces and Training

A critical part of this new initiative will be the formation of Counter-Proliferation Task Forces in appropriate U.S. Attorney's offices around the country. These multi-agency task forces will take many of the concepts used in combating terrorism – namely, prevention, cooperation and coordination -- and apply them to the counter-proliferation effort. The task forces will be designed to enhance cooperation among all agencies involved in export control, forge relationships with affected industries, and facilitate information sharing to prevent illegal foreign acquisition of U.S. technology.

The Department's National Security Division is in discussions with districts with large concentrations of high-tech businesses and research facilities -- all of which are potential targets for illegal foreign acquisition efforts -- as potential venues for new task forces. Some task forces may be modeled after efforts that exist in the Southern District of New York, District of Connecticut and District of Maryland, where agents from ICE, FBI, Commerce Department, DCIS and other agencies pool data and coordinate cases. Other approaches may be taken in different districts, depending on the needs of the U.S. Attorney and agencies in that district.

The new initiative also includes key training components. Export prosecutions are by nature complex because they involve intricate laws, sensitive international issues, agencies with different authorities, and, often, classified information. Under the initiative, the Department will provide specialized training to its field prosecutors, especially those with limited expertise in export control. The Department launched this enhanced training effort in May with a national conference in South Carolina.

The Justice Department has also appointed its first National Export Control Coordinator to implement this initiative and foster coordination among the agencies involved in export control. Based in the Counterespionage Section of the National Security Division, the Coordinator is responsible for managing the nationwide training of prosecutors and monitoring progress on export control prosecutions around the country.

Improved Coordination With Export Licensing Agencies

A final component of the initiative involves greater coordination between the Justice Department and the export licensing agencies, particularly the State Department's Directorate of Defense Trade Controls and the Commerce Department's Bureau of Industry and Security. As part of the initiative, the Justice Department's National Security Division has initiated monthly meetings with the leadership of these offices to ensure that investigations, prosecutions and enforcement issues are fully coordinated.

"These crimes result in some of the most complex and time-consuming cases facing federal law enforcement," said Julie L. Myers, Homeland Security Assistant

Secretary for ICE. "The concept of terrorists, criminals or rogue nations obtaining weapons and other restricted technology is chilling. By harnessing our collective authorities and efforts, we are better able to protect our national security and global public safety."

According to Timothy D. Bereznay, Assistant Director, FBI Counterintelligence Division, "The FBI is committed to working with our law enforcement and intelligence partners in the aggressive pursuit and investigation of high technology export violations. The theft of intellectual property and technology by foreign parties or governments directly threatens both the national and economic security of the U.S. in which the development and manufacturing of U.S. products results in weakened economic capability and diminished political stature for this country."

"I commend Assistant Attorney General Wainstein and the Department of Justice for their leadership on the Export Enforcement Initiative," said Commerce Assistant Secretary for Export Enforcement Darryl W. Jackson. "This initiative enhances the administration's counter-proliferation program by vigorously pursuing and prosecuting individuals who violate our laws and allow U.S. technology to fall into the wrong hands."

"There are few greater threats to our soldiers, sailors, airmen, and marines than confronting highly-advanced weapons and technology which were designed to protect them and to give them the advantage on the battlefield. It is clear then why the Defense Criminal Investigative Service has for years made illegal technology export a top investigative priority. Our agents, who are dedicated to protecting America's Warfighters, need no motivation in aggressively pursuing these criminals. This initiative is vital and has our full support," said DCIS Director Charles W. Beardall.

"As head of the U.S. Government agency responsible for controlling the export of U.S. defense articles and services, I am delighted to lend my full support to the Export Enforcement Initiative. The Department of State has always maintained a close, working relationship with the federal law enforcement community in its investigation and prosecution of criminal violations of our nation's export control laws. We expect that relationship to only become stronger under this initiative to keep sensitive defense items out of the wrong hands," said Acting Assistant Secretary of State Stephen D. Mull.

Foreign Efforts to Obtain Controlled U.S. Technology

The technology at the heart of this initiative includes restricted U.S. military items, dual-use equipment, and other technical expertise or know-how, some of which have applications in Weapons of Mass Destruction (WMD). These materials are generally restricted and may not be exported without U.S. government approval. Foreign procurement networks intent on obtaining such materials from the U.S. rarely target complete weapons systems, but often focus on seemingly innocuous components to develop their own weapons systems. Two cases in the past week are exemplary:

- ***Nuclear-Related Technology to Pakistan*:** On Oct. 4, 2007, a Pittsburgh company called SparesGlobal, Inc. was sentenced in the Western District of Pennsylvania for conspiring to make false statements about an illegal export of graphite products that can be used in nuclear reactors and in the nose cones of ballistic missiles. These sensitive products ended up in Pakistan after being routed through the United Arab Emirates. The investigation was conducted by Commerce Department agents.

- ***Illegal Exports of U.S. Fighter Jet Components*:** On Oct. 5, 2007, Abraham Trujillo and David Wayne were charged in the District of Utah with attempting to illegally export restricted components for F-4 and F-14 fighter jets. Such exports are of particular concern because F-14 components are widely sought by Iran, which is currently the only government in the world that still flies the F-14 fighter jet. The investigation was conducted by ICE and DCIS agents.

According to the Intelligence Community's most recent report to Congress on Foreign Economic Espionage and Industrial Collection, private-sector businessmen, scientists, students, and academics from overseas are among the most active collectors of sensitive U.S. technology. Most did not initially come to the U.S. with that intent, nor were they directed to do so by foreign governments. Instead, after finding that they had access to technology in demand overseas, they engaged in illegal collection to satisfy a desire for profits, acclaim, or patriotism to their home nations.

At the same time, foreign government organizations remain aggressive in illegally acquiring sensitive U.S. technology. Some governments have established quasi-official organizations in the U.S. to facilitate contact with overseas scientists, engineers and businessmen. Foreign governments have been observed directly targeting U.S. firms; employing commercial firms in the U.S. and third countries to acquire U.S. technology; and recruiting students, professors, and scientists to engage in technology collection.

Enhanced U.S. Law Enforcement Response

In addressing such threats, law enforcement agencies and federal prosecutors have stepped their enforcement activity in recent years. ICE has recently doubled the number of agents assigned to export control cases and reports making 149 export-related arrests last fiscal year. The FBI reports that it is investigating roughly 125 economic espionage cases and has increased counterintelligence instruction for new agents by 240 percent.

The Commerce Department reports that more than 80 percent of its export convictions in fiscal year 2007 were related to WMD proliferation, terrorist support or diversion to military end-use. DCIS and other Defense Department agencies have also stepped up their investigative efforts to protect critical military technologies. As a result, the Justice Department has seen a corresponding surge in export prosecutions. In fiscal year 2007, there was more than a 50 percent increase in defendants charged with violating the primary export control statutes compared to the prior year.

###

07-806