NASA KSC Export Control Office (ECO) 1105 HQ
On the web at http://*exportcontrol.ksc.nasa.gov*
EC Hotline (321) 867-9209

KSC Export Control Brief



JANUARY - MARCH 2012

THE FOCUS: Real-Life Case$ of ITAR Violation$ + the Penalties

THE ITAR MYSTERY? THE FACTS….

The ITAR regulates Defense Articles, Defense Services, and Technical Data listed on the U.S. Munitions List (USML).

KSC Defense Articles on the USML: Space Shuttle, rocket acoustic prediction S/W, Atlas vehicle, Pad A, and more.

Defense Services means giving assistance (including training) to foreign nationals when it's related to defense articles and tech data.

Tech Data means information for the design, development, production, operation, testing, or maintenance of defense articles.

Inside this issue

SHUTTLE TILES STOLEN BY FORMER KSC USA EMPLOYEE

From the 2011 Officer of the Inspector General (OIG) annual report to Congress — An OIG investigation was initiated when an individual purchased a Space Shuttle Thermal Protection System tile on eBay and submitted a Freedom of Information Act (aka FOIA) request to NASA to determine the origin of the tile. OIG investigators subsequently traced the tile, subject to the ITAR, to a former USA employee at Kennedy Space Center. The OIG determined that the employee had sold 12 stolen Space Shuttle tiles on eBay for prices ranging from $41 to $912. He was charged with third degree felony theft and trafficking in stolen property, sentenced to 12 months of probation, ordered to pay $5,353 in restitution and $742 in fines and fees, and perform 50 hours of community service.

DON'T BE THIS GUY: FORMER NASA ENGINEER PLEADS GUILTY TO ILLEGAL MILITARY EXPORTS

Kue Sang Chung, 66, who retired in 2008 after 25 years with NASA, pled guilty in January 2011 to illegally exporting infrared military technology to South Korea. On January 20, 2011, the longtime employee at NASA Glenn Research Center in Ohio pleaded guilty in the Northern District of Ohio to one count of violating the Arms Export Control Act and one count of filing false tax returns. He admitted to misusing his NASA position. Prosecutors said he claimed he was operating under a subcontract with NASA and had permission to buy 13 restricted components from a NJ-based business. He then resold the items to the South Korean contractor.

According to court documents, while working as an electrical engineer for NASA, Chung also operated a business out of his home

(Continued p. 2, "Former NASA Engineer Pleads Guilty")

ECO Mission: Protecting NASA technologies & KSC employees through the enforcement of federal import-export regs

TRAVELING "ELECTRONICALLY NAKED" IN AN AGE OF DIGITAL ESPIONAGE

The New York Times, Feb 10, 2012

When Kenneth Lieberthal, a China expert at the *Brookings Institution, travels to China, he follows a routine that seems right out of a spy film. He leaves his cell phone and laptop at home and brings company "loaner" devices which he erases before leaving the U.S., then wipes clean the moment he returns. In China, he disables Bluetooth and Wi-Fi, never lets his phone out of sight, and not only turns off his phone in meetings but also removes the battery for fear the phone's microphone could be turned on remotely. He connects to the internet only through an encrypted, password-protected channel, and he copies and pastes his password from a USB thumb drive. He never types a password in directly because "the Chinese are very good at installing key-logging software on your laptop."

This once paranoid behavior is now standard operating procedure for American government officials doing business in China and Russia — like Google, the State Department, and Internet security giant McAfee. Anyone having significant intellectual property that the Chinese and Russians want, and you go there with mobile devices, your devices will get penetrated, according to Joel Brenner, former top counterintelligence official from the office of the director of national intelligence.

Both China and Russia prevent travelers from entering the country with encrypted devices without government approval. Several U.S. companies and government agencies are doing the same by imposing do-not-carry rules. McAfee said that if any employee's device was inspected at the Chinese border, it could never be plugged into McAfee's network again. Ever. It has become easier to steal information remotely because of the Internet, the proliferation of smartphones, and the inclination of employees to plug their personal devices into workplace networks and cart proprietary information around. "We've already lost our manufacturing base," said Scott Aken, former FBI agent specializing in counterintelligence and computer intrusion. "Now we're losing our R&D base. If we lose that, what do we fall back on?"

**Brookings, considered the #1 think tank in the world, is a nonprofit public policy organization based in Washington, D.C. The mission is to conduct high-quality, independent research in policy-oriented public policy, international development, domestic economic policy, and social policy to advance the goals of safe international cooperation and strengthening American social welfare, security, and democracy.*

("Former NASA Engineer Pleads Guilty")

through which he illegally exported U.S. munitions to South Korea and performed consulting services for Korean businesses. He illegally exported several infrared focal plane array detectors and infrared camera engines to South Korea for use in Korean government projects between March 2000 and November 2005. These items are classified as defense articles on the U.S. Munitions List, and a State Department license is required for their export. Chung entered into a contract with a Korean company to design, build, and text electronics to support the items he was exporting. On occasion, he used his NASA e-mail address to order sensitive items from U.S. manufacturers, falsely asserting that they would be used for NASA projects in the United States, when in fact they were to be exported to South Korea.

Chung received about $200,000 for the components and for his services to design, build, and test the electronics to support infrared research. The engineer was sentenced in November 2011 to 14 months in prison, far below federal sentencing guidelines. Because he failed to report the income to the Internal Revenue Service, he must pay about $40,000 in unpaid taxes plus interest and penalties as part of his sentence. Chung is divorced from his wife and sleeps on a cot in his Avon Lake, OH office, where he runs a consulting business. The investigation was conducted by the FBI and IRS.

SPOTLIGHT ON HEATHER WHITE

EXPORT CONTROL/COMPLIANCE & SECURITY MGT OFFICER ENGINERING SERVICES CONTRACT (ESC—TEAM QNA)

My adventure in export control began in 2009 when I made a career change. I was a Litigation Paralegal in the areas of commercial contracts, civil, and bankruptcy for 12 years and was starting to feel burned out. I really enjoyed being a Paralegal but wanted to learn something new, more exciting, and still be able to use my legal skills and knowledge.

In August 2009, I joined the export control office of ASRC Aerospace and soon became an "export control specialist". I worked with two others and was responsible for conducting export control reviews, providing export control overviews to employees, and giving foreign travel briefings to employee travelers, among other tasks that came with the territory. As the ASRC engineering services contract approached the end, my two co-workers left to join other companies. Being new in the field and wanting to stay on the Space Coast, I joined Stinger Ghaffarian Technologies (SGT, Inc.) in February 2011 on the new Engineering Services Contract (ESC – Team QNA), only to learn that I would be their sole Export Control/Compliance Officer and Security Management Officer. Wow, nothing like being thrust right into the thick of things! I am now responsible for all ESC requirements with regard to export control and security. I focus on all reviews for export-controlled and Sensitive But Unclassified material, and OCI on task orders. I am also responsible for reviewing shipments, training ESC employees on export control, SBU and OCI, ESC foreign national visitors, ESC foreign travel and many other export control and security activities.

At the start of the ESC, I incorporated KSC Form 7-657 developed by the NASA ECO for documenting the export determination and SBU status of hardware, technical documents, and drawings. By doing this, I work daily with the NASA Export Control Office and have built an excellent rapport with them. In May 2011, I traveled with the NASA ECO to my first NASA HQ Export Control Program Review, hosted by NASA Glenn Research Center in Cleveland, and I will be attending the 2012 Program Review at NASA Ames Research Center in California.

When I began my new adventure in export control, I wasn't quite sure what I was getting myself into. I absolutely love my job! I love that each day brings a new challenge and have found field of export control to be rewarding.

I value the experience that I acquired through my years as a Paralegal and now as an export compliance officer, but I credit my education with helping me achieve success in my career. I graduated from King's College (Charlotte, NC) with a Certificate, Legal Studies, in May 1999, then from Everest University (Orlando, FL) in October 2008 with a Bachelor of Science, Paralegal. I have also had the opportunity to obtain certifications along the way. In April 2010, I became a Certified U.S. Export Compliance Officer (CUSECO®) through the International Import-Export Institute. I recently completed the EAR/ITAR Export Compliance Professional (ECOP-EAR® / ECOP-ITAR®) through the Export Compliance Training Institute.

When I am not at work, I enjoy being outdoors. I love being out on the water boating and fishing, going out on the 4-wheelers, and riding on my husband's Harley (the picture is his old Harley). I also enjoy spending time with my two dogs and cat.

-Heather White

Office phone: (321) 867-6632
Internal mail: Mail Code ESC-16
E-mail: heather.r.white@nasa.gov
Snail mail: P.O. Box 21014, Kennedy Space Center, FL 32815

Need a drawing or technical document marked for export control? Use KSC Form 7-657, attach your file, and e-submit.

ITAR VIOLATIONS Arms Export Control Act

BACKGROUND

The U.S. does not tolerate indiscriminate arms transfers, so it strictly regulates export and re-exports of defense items and technologies to protect its national interests and international community interests in peace and security. The U.S. Government views the sale, export, and re-transfer of defense articles and defense services as an integral part of safeguarding U.S. national security and furthering U.S. foreign policy objectives.

TENNESSEE MAN PLEADS GUILTY TO ILLEGALLY EXPORTING BULLET PROOF VESTS

Released January 13, 2011 by Department of Justice

Jerome Stewart Pendzich, 34, of Hampton, TN, pleaded guilty in United States District Court to knowingly exporting a defense article without a license or approval from the State Department. This is a violation of the Arms Export Control Act, which carries a maximum possible penalty of 10 years in prison, a $1,000,000 fine and 3 years supervised release.

According to the information and plea agreement, in January 2009, special agents from Immigration and Customs Enforcement (ICE) became aware that Pendzich was attempting to sell a certain type of bullet-proof vest on eBay that is prohibited from export by law. Further investigation revealed that in May and June of 2009 he attempted to ship export-controlled small arms protective inserts (SAPI plates) to "customers" in Bogotá, Columbia, South America. Pendzich had previously been advised by his supplier that an export license from the U.S. State Department was required before he could attempt to send the SAPI plates overseas. Those "customers" turned out to be federal undercover agents who had placed orders for fake customers, with other agents waiting in Bogotá to take delivery of shipments that Pendzich had labeled as "gifts" and "ceramic plates".

His attorney argued that his client's actions did not actually threaten national security because only federal agents, not potential terrorists, physically received the shipments. However, the U.S. District court judge on the case found that the defendant's conduct had the potential to cause harm to the interests of the United States. The judge denied probation and sentenced Pendzich to 46 months in federal prison for violating the Arms Export Control Act, which requires government approval for foreign sales and distribution of military equipment listed on the U.S. Munitions List in the ITAR.

STOLEN NIGHT VISION & OPTICS TO CHINA AND ENGLAND

Released by Department of Justice

In November 2011, Phillip Andro Jamison, a former Gunner's mate Petty Officer First Class in the U.S. navy stationed about Naval Amphibious Base Coronado, was sentenced to serve 30 months in prison for violating the Arms Export Control Act. The indictment 1 year earlier alleged that while working in his unit's armory, he stole more than 280 items from the Navy and sold them to customers via eBay. He admitted stealing combat-grade night vision devices, riflescopes, and laser aiming devices and illegally exporting them to Hong Kong, without first obtaining the required export licenses from the State Department.

MILITARY TECH DATA TO CHINA

Released by Department of Justice

Steve Liu, a native of China with a doctorate degree in electrical engineering and an 18-month senior staff engineer for Space & Navigation, a division of L-3 Communications in New Jersey, was arrested in March 2011 and charged with one count of exporting defense-related technical data without a license. He was part of the L-3 team that worked on precision navigation devices for the DoD. In November 2010, the month he was terminated from L-3, he traveled to China and, upon his return to the U.S., Customs and Border Patrol inspectors found him to be in possession of a computer that contained hundreds of documents related to company projects and images of himself making a presentation at a technology conference sponsored by the government of the People's Republic of China. Liu had never been issued a company laptop. Nor was he approved to possess the company's work product outside the NJ facility. Many of the documents on the computer were marked as company proprietary and/or export-controlled tech data. The State Department certified that information on the computer was export-controlled technical data under the ITAR that relates to defense items on the U.S. Munitions List.

ITAR violations based on illegal e-Bay® sales of export-controlled items are on the rise. Don't let it happen to you.

("ITAR Violations" continued)

MASSACHUSETTS MAN PLEADS GUILTY TO CONSPIRACY TO EXPORT MILITARY ANTENNAE TO SINGAPORE AND HONG KONG

Released January 20, 2012 by U.S. Department of Justice, United States Attorney's office

WASHINGTON - Rudolf L. Cheung, 57, a resident of Massachusetts, pleaded guilty today in federal court in the District of Columbia to conspiracy to violate the Arms Export Control Act in connection with the unlawful export of 55 military antennae from the United States to Singapore and Hong Kong.

The plea was announced by Lisa Monaco, Assistant Attorney General for National Security, and a team of top government officials from Department of Commerce, FBI, Homeland Security, and the U.S. District of Columbia.

Cheung serves as the head of the Research & Development department at a private company that manufactures antennae. Over the past 17 years, he has designed or supervised the development of a full library of antennae made by the firm, many of which have military applications and are used by defense contractors. Some of Cheung's inventions are used in the U.S. space program.

According to court documents filed in the case, in June 2006, a company in Singapore sent an inquiry to the firm that employs Cheung seeking a quotation for 2 types of antennae that are classified by the U.S. government as defense articles and may not be exported without a license or approval from the State Department. After receiving the query, the export compliance officer at Cheung's firm advised the firm in Singapore that neither antenna could be exported unless they filled out a U.S. government form attesting that the goods would not be transferred. The firm in Singapore refused and the order was stopped.

After learning that the export compliance officer at his company had blocked the export, Cheung admitted that he discussed with an individual outside his company (co-conspirator C) a plan to bypass the export controls at his company and arrange for the antennae to be exported to Singapore through co-conspirator C. Under the plan, co-conspirator C, who operated his own company in Massachusetts, would purchase these goods from Cheung's company and then export them on his own to the firm in Singapore, with Cheung's knowledge. Subsequently, co-conspirator C contacted the firm in Singapore and offered to broker the deal with Cheung's company. Co-conspirator C then negotiated the purchase of the antennae with employees of the firm in Singapore and, later, with another company called Corezing International in Singapore. Between July and September 2007, co-conspirator C purchased 55 military antennae from Cheung's company, which he then exported to Corezing addresses in both Singapore and Hong Kong.

According to court documents, Cheung was aware that the purchases by Co-conspirator C were intended for export from the United States and that these exports had previously been blocked by his export compliance manager. Yet Cheung took no action to stop the sale of these antennae from his company or their subsequent export from the United States, even though he knew a license was required for such exports. Cheung neither sought nor obtained any license from the State Department to export these items outside the United States.

At sentencing, Cheung faces a maximum potential sentence of 5 years in prison, a fine of $250,000 and a 3-year term of supervised release.

Corezing (and its principals), based in Singapore, have been charged in a separate indictment in the District of Columbia in connection with the export of these particular military antennae to Singapore and Hong Kong. The United States is seeking their extradition, in connection with the export of 6,000 radio frequency modules from the United States to Iran via Singapore, some of which were later found in improvised explosive devices in Iraq.

- SEE THE ECO TEAM -

CEA
Wayne Ranow

Associate CEA
Melanie Chan

Specialists
Doug Lesho
Dave Baptiste

In keeping with NASA Center trends, the Export Control Office was returned to the Ops Support Division of TA with logistics, property, and transportation.

Still same location and same great service!

ARE YOU EXPORT COMPLIANT?

YOU SHOULD BE…. IT'S THE LAW!

FAQs 102
THE ITAR

Explain what this ITAR stuff is.

Arms Export Control Act of 1976 (AECA) gives the President of the United States the authority to control the import and export of defense articles and defense services.

International Traffic in Arms Regulations (**ITAR**) is a set of U. S. government regulations that controls the export and import of defense-related articles and defense services on the United States Munitions List (USML).

The **ITAR** implements the provisions of the AECA, and the ITAR regs are described in the Code of Federal Regulations: Title 22 (Foreign Relations), Chapter I (Department of State), Subchapter M.

The **Directorate of Defense Trade Controls** (DDTC under Department of State) interprets and enforces the ITAR.

For practical purposes, ITAR regs dictate that material pertaining to defense/military related technologies may only be shared with U.S. Persons unless authorization from the Department of State is received or a special exemption is used.

For the benefit of us researchers and engineers, what are some examples of "exports" that we may encounter?

- ⇨ Transfers of technical data to persons and entities anywhere in the world
- ⇨ Shipment of controlled items, such as scientific equipment, that require export licenses, from the USA to a foreign country or foreign person
- ⇨ Providing a defense service (furnishing of assistance, including training) to foreign persons everywhere
- ⇨ Verbal, written, electronic, or visual disclosures of controlled scientific and technical information to foreign nationals in the U.S.… aka "deemed export"

I just want to personally send something overseas to a fellow researcher I met at a conference. Do I need to worry about whether or not my item needs a license to ship?

You still need to determine whether or not an export license is required, even if it's a gift and no sales are involved. Don't worry, but please ask someone in the Export Control Office for help. If you need a license, NASA HQ will help us get it for you. With luck, we may be able to locally provide a License Exemption for your "export" instead of having to wait for a License from State Dept.

What's the rationale behind regulating defense exports?

The U.S. Government views the sale, export, and re-transfer of defense articles and defense services as an integral part of safeguarding U.S. national security and furthering U.S. foreign policy objectives. The U.S. does not tolerate indiscriminate arms transfers, so it strictly regulates export and re-exports of defense items and technologies to protect its national interests and international community interests in peace and security.

What can happen if I don't get the proper export authorization?

Responsibility for export compliance is with the exporter, meaning YOU. U.S. Persons and organizations can face heavy $$$ fines, imprisonment, or both, if they have, without authorization or exemption, provided foreign persons with access to ITAR-protected defense articles, services, or technical data.

At an AIAA conference, my co-worker gave an export-controlled report to a Chinese physicist (living in FL). Oops??

If your office was involved in a violation of the ITAR, please tell the ECO asap! We have a chance to submit a Voluntary Self Disclosure, an important indicator of our intent to comply. The KSC ECO will assist NASA HQ, who will report the violation to Department of State.

John F. Kennedy Space Center

Export Control Brief

"Export Control Brief" has been published by the NASA Export Control Office, Protective Services (TA-A2), for KSC civil servant and contractor employees. Contributions are welcome at anytime and may be sent to Melanie Chan at ***melanie.r.chan@nasa.gov.***

ITAR, Official Version, Published April 1, 2011 - - http://pmddtc.state.gov/regulations_laws/itar_official.html