THE REGENTS OF THE UNIVERSITY OF CALIFORNIA
OFFICE OF ETHICS, COMPLIANCE AND AUDIT SERVICES

Top Ten Things You MUST Know -

Before Taking your Laptop Overseas

Brian Mitchell Warshawsky
Systemwide Export Control Officer

ECAS Webinar Series
Wednesday May 15th, 2013

In the news… Sept. 26, 2012:

- A federal jury in Newark found Steve Liu guilty on nine counts, including exporting defense-related data without a license, possessing stolen trade secrets and lying to federal agents.
- The case began when he was stopped with his laptop at Newark Airport on his return from China.
- FBI's Top Ten News Stories for the Week Ending September 28, 2012

The Threat

- While in the PRC, Liu gave presentations at several universities…
- Prosecutors admit no knowledge of what was said at those presentations.
- For the export crimes he was convicted of, he only had to have taken certain defense articles or data outside the United States without a license or other approval from the State Department.

The Case

- **Sixing "Steve" Liu was stopped by U.S. Customs and Border Protection officers on Nov. 29, 2010, after flying back from a speaking engagement at a highly technical nanotechnology conference hosted by local universities and Chinese government officials.**
- **Apparently, border agents' suspicions were aroused when the agents found a conference lanyard in his luggage during a secondary inspection at New Jersey's Newark Liberty International Airport. Liu had said he'd been in China to visit family.**
- **Border guards also found a laptop. After obtaining a search warrant, federal investigators then discovered hundreds of company documents on Liu's computer, including several that contained technical data on guidance and control systems governed by U.S. arms export control laws.**
- **According to his LinkedIn profile, Liu's area of expertise at L-3 Communications was building very small-scale measurement systems using what's called MEMS (micro-electro-mechanical system) technology. MEMS chips are hot right now: They're what Apple's iPad uses to know how it's being moved around by game-players. Liu was using them to build complex aerospace navigation systems.**
- **The U.S. Department of Justice described Liu's presentation at the 4th Annual Workshop on Innovation and Commercialization of Micro & Nanotechnology as a "presentation sponsored by the Chinese government.“**
- **and government and scientific agencies, including China's Ministry of Science and Technology.**
- **Liu had spoken at the conference more than once. He was a co-chairman of the event in 2009 and gave a talk entitled "Micro-Navigator for Spacecraft with MEMS Technology" at that year's event. He had been working for L-3 Communications for about seven months at the time of the 2009 workshop.**

Media Reporting

THE AUSTRALIAN | LOGIN | SIGN UP

NEWS

NEWS OPINION NATIONAL AFFAIRS BUSINESS AUS IT HIGHER ED MEDIA SPORT ART

BREAKING NEWS | THE NATION | THE WORLD | FEATURES | IN-DEPTH | GALLERIES | INVESTIGATIONS

THE WORLD

Recommend 2

US man Sixing Liu 'sold military secrets' to China

AP September 27, 2012 11:29AM

A FORMER employee of a New Jersey-based defence contractor has been foun of taking US military technology trade secrets from his employer and exporting his native China.

Sixing Liu, also known as Steve Liu, worked for Space & Navigation, a New Jersey division of New York-based L3 Communications. Liu, who had lived until recently in Flanders, New Jersey, was arrested at his home in Deerfield, Illinois, in March 2011 and accused of taking restricted military data and presenting them at two conferences in China the previous fall.

Prosecutors argued the technology was proprietary and could be used for target locators and other military applications.

A federal jury in Newark found Liu guilty on nine counts, including exporting defence-related data without a licence, possessing stolen trade secrets and lying to federal agents.

He was acquitted on two counts of lying to federal authorities about one of his visits to China.

Ocean County
Family & Community News
Toms River • Brick • Jackson • Manchester • Lakewood • Berkeley • Lak

HOME | BUSINESS | COMMUNITY | EVENTS | FIRE & SAFETY | NEWS | OPINI

About | Our Services | Submit News | Advertise | Help Wanted

Monday, September 24th, 2012 | Posted by Toms River, NJ

In the Courts: Closing Arguments to be Held in New Jersey Spy Case

9:30 a.m. – Closing arguments, U.S. v. Liu – Closing arguments in the trial of Sixing Liu, a/k/a, "Steve Liu," 48, of Deerfield, Ill., and recently of Flanders, N.J., a former employee of a New Jersey-based defense contractor, for allegedly misappropriating and exporting sensitive military technology to the People's Republic of China (PRC) – before Judge Chesler (Newark)

Media Reporting

examiner.com

Google

News & Info | Business | Politics | News | Sports | Science & Space | Video | More

Defense contractor's worker stole military technology for China

MILITARY ESPIONAGE | SEPTEMBER 29, 2012 | BY: JIM KOURI | + Subscribe

Published On: Thu, Sep 27th, 2012

Military News | B

Chinese Male Convicted In US Troops Info Case

NEWARK, New Jersey (AP) — A former worker of a New Jersey-based invulnerability executive w found guilty Wednesday of holding U.S. troops record trade secrets from his employer and export them to his local China.

The Cutting Edge

Wednesday February 06 2013

Investigation | Slices | Energy | Security | Analysis | Arts | Travel | Resou

The Weapon's Edge Back

Defense Contractor's Worker Stole Military Technology for China

Jim Kouri September 29th 2012

Examiner

A jury on Thursday convicted an employee of a defense contractor for exporting sensitive U.S. military technology to the People's Republic of China (PRC), stealing military secrets, and making false statements to federal law enforcement.

Sixing Liu, a/k/a "Steve Liu," a Chinese citizen who lived in Flanders, New Jersey, and in Deerfield, Illinois, was immediately taken into federal custody after the jury announced their verdict. U.S. District Judge Stanley R. Chesler based his decision for Liu to remain in custody after agreeing with the prosecutor that Liu was a flight risk. Sentencing before Judge Chesler is scheduled for Jan. 7, 2013.

The Conviction…

…made the FBI's Top Ten News Stories for the Week Ending September 28, 2012

At sentencing…

- Liu received 70 months in prison
- Prosecution sought 97 months or more
- Liu “I was trying to help the students with the new technology”
- Judge: “…even today there is not the slightest indication that you understand what you did.”

Goals

Share a framework for understanding the regulatory framework and rules applicable to laptop travel

Alert you to recent trends

Share available resources and best practices

Which of the following constitutes an “Export”?

1. A researcher takes their laptop abroad to aid in their research.
2. A researcher allows a foreign national to participate in their research within the U.S.
3. A researcher allows a foreign national to access their laptop overseas.
4. A researcher returns an Inertial Navigation Instrument to his foreign colleagues by stowing it in his carry-on luggage.

All examples are exports!

"'Export' means an actual shipment or transmission of items subject to the EAR* out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States"

- *Export Administration Regulations (EAR)

Areas Subject to Export Controls

- Direct export of a controlled item
- Foreign national access/use of controlled item
- Foreign travel to a restricted country
- International and domestic collaborations
- Publications (that are not generally accessible to public)
- International and domestic presentations at conferences
- Conversations involving controlled technology
- Taking or shipping a controlled item out of the U.S.

10

YOU…
Are an Exporter!

- Your travel activities may legally constitute an export
- Hand-carry travel items such as your laptop, PDA/cellphone, and software are subject to export controls.

All are exports…

- A U.S. citizen instant messages a South Korean national working together in New York City about technical drawings for items controlled under U.S. export regulations.
- A U.S. employee emails to India software updates necessary to operate an item controlled under U.S. export regulations.
- A professor at Harvard University lectures in China on her research relating to a project with technology controlled under U.S. export regulations.

Exports may require a License #9

Taking certain items outside the US “may” require a license, for example:

- Controlled technology
- Controlled hardware
- Data, technology
- Blueprints, schematics

Licensing Agencies

The U.S. federal government agencies responsible for implementing export control regulations are:

- Department of Commerce
  - **Export Administration Regulations (EAR)**
  - Applies to "dual-use" technologies; technical data and commodities that have both commercial and military/security applications
- Department of State
  - **International Traffic in Arms Regulations (ITAR)**
  - Applies to inherently military/satellite technologies or items that can be used in a defense/military application
- Department of Treasury
  - **Office of Foreign Assets Control (OFAC)**
  - Prohibits transactions with countries subject to boycotts, trade sanctions, embargoes, and/or restricted persons

ENFORCEMENT! #8

- Increasing government scrutiny post 9/11
  - Growing intersection of science, technology and engineering research with national security, foreign policy and homeland security
  - Roles of universities and shifting research projects

- Severe criminal and civil noncompliance penalties and sanctions for individuals as well as institutions/corporations
  - Up to $1M for institutions/corporations and up to $250,000 for individuals
  - Up to 10 years in prison
  - Termination of export privileges
  - Suspension and/or debarment from federal government contracting
  - Loss of federal funds

COUNTERINTELLIGENCE

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE

FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE

Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011

October 2011

Federal Focus on Laptops

Intelligence Note
Prepared by the
Internet Crime Complaint Center (IC3)
May 8, 2012

MALWARE INSTALLED ON TRAVELERS' LAPTOPS THROUGH SOFTWARE UPDATES ON HOTEL INTERNET CONNECTIONS

Recent analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while establishing an Internet connection in their hotel rooms.

Recently, there have been instances of travelers' laptops being infected with malicious software while using hotel Internet connections. In these instances, the traveler was attempting to setup the hotel room Internet connection and was presented with a pop-up window notifying the user to update a widely-used software product. If the user clicked to accept and install the update, malicious software was installed on the laptop. The pop-up window appeared to be offering a routine update to a legitimate software product for which updates are frequently available.

The FBI recommends that all government, private industry, and academic personnel who travel abroad take extra caution before updating software products on their hotel Internet connection. Checking the author or digital certificate of any prompted update to see if it corresponds to the software vendor may reveal an attempted attack. The FBI also recommends that travelers perform software updates on laptops immediately before traveling, and that they download software updates directly from the software vendor's Web site if updates are necessary while abroad.

Anyone who believes they have been a target of this type of attack should immediately contact their local FBI office, and promptly report it to the IC3's website at www.IC3.gov. The IC3's complaint database links complaints together to refer them to the appropriate law enforcement agency for case consideration. The complaint information is also used to identify emerging trends and patterns.

Applicable Law Enforcement Agencies

- Federal Bureau of Investigation
- Immigration & Customs Enforcement
- Department of Commerce
- Air Force Office of Special Investigations
- Defense Criminal Investigative Services
- Naval Criminal Investigative Services
- Alochol, Tabacco & Firearms
- United States Secret Service
- Customs & Border Protection
- Drug Enforcement Agency
- Intelligence Agencies (CIA, DIA, NSA, etc.)
- Army Criminal Investigation Command
- Others too

Evidence….

- Shipper's Export Declarations: Who completes them? Have they been interviewed?
- Immigration Records: A-File, I-129 (Part 6)
- Subsidiary or Affilate websites
- Interview by CBP at Port of Entry
- Suspicious Activity Reports (SARS)
- Rule 41 Search Warrant on Email
- End-User Forms BIS 711 Forms
- Undercover Platforms
- Voluntary Self-Disclosures
- No Action or Cautionary Letters Sent by OFAC, BIS or DDTC
- FISAs
- Undercover Platforms
- Subpoena to Freight Forwarder
- Subpoena to Bank
- Border Search for Electronic Devices
- Cell phone text messages
- Designations or public information about companies
- Denied license application
- Invoices & Air Waybills
- Secretary of State Websites
- Industry Outreach
- Attendance or Presentation at Export Conferences
- Customs to Customs request to foreign partners (CMAAs)
- Post-Shipment or Pre-Shipment Verifications (BIS/Embassy Officers)

Border Search Exception to the 4th Amend.

Searches conducted at the United States border or the equivalent of the border (such as an international airport) may be conducted without a warrant or probable cause subject to the "border-search" exception

Laptop Rule:

The U.S. Courts of Appeals for the Fourth and Ninth circuits have ruled that information on a traveler's electronic materials, including personal files on a laptop computer, may be searched at random, without suspicion (US v. Ickes, 393 F.3d 501 (4th Cir., 2005) & US v. Arnold, 523 F.3d 941 (9th Cir. 2008)

Newest case: US v. Cotterman....

Border Search Exception to the 4th Amend.

Trends and Developments

- "Exports" include the "click of the mouse": Broadening of investigations to include new industries and new aspects of business.
- More Cases: FBI Director Mueller, July 2012: "We now have more than 1,500 pending [export control] cases, and in the past year, we made several high-value arrests and witnessed a significant increase in disruptions."
- DHS Director Morton, June 2012: "In fiscal year 2011, HSI special agents initiated a total of 1,785 criminal investigations into possible export violations, made over 530 arrests, and obtained 487 indictments and 304 convictions for export related criminal violations."

Destination matters #7

Federal agencies maintain numerous lists with rules which vary by country

Not All Foreign Countries are treated equally

Sanctioned countries

Cuba, North Korea, Iran, Syria, Sudan

Secondary lists… based on the controls applicable to individual exports…

Import Restrictions too?

Countries with encryption import and use restrictions

- Burma (you must apply for a license)
- Belarus (import and export of cryptography is restricted; you must apply for a license from the Ministry of Foreign
- Affairs or the State Centre for Information Security or the State Security Agency before entry)
- China (you must apply for a permit from the Beijing Office of State Encryption Administrative Bureau)
- Hungary (import controls)
- Iran (strict domestic controls)
- Israel (personal-use exemption – must present the password when requested to prove the encrypted data is
- personal)
- Morocco (stringent import, export and domestic controls enacted)
- Russia (you must apply for a license)
- Saudi Arabia (encryption is generally banned)
- Tunisia (import of cryptography is restricted)
- Ukraine (stringent import, export and domestic controls)

What's in your wallet? #6

Transporting a computer that has encryption software installed is subject to a number of controls.

The U.S. Department of Commerce and the Department of the Treasury both have rules designed to control the movement of encryption technology out of the United States. The Department of Commerce's Bureau of Industry and Security and the Office of Foreign Assets Control (OFAC) within the Department of the Treasury accept applications for licenses to export encryption products and technologies.

The Departments of Defense, Justice and State also have the right to review license applications. The review can take about 90 days and in some cases longer

Technology specifics are critical

- Difference between Commercial Off the Shelf Software (COTS) and proprietary or unreleased software

- Unpublished Research Data if not covered under the FRE

- Adjusted Peak Performance (APP) is a metric introduced by the U.S. Department of Commerce's Bureau of Industry and Security (BIS) to more accurately predict the suitability of a computing system to complex computational problems, specifically those used in simulating nuclear weapons. This is used to determine the export limitations placed on certain computer systems under the Export Administration Regulations

- Hardware - Specialty laptops and equipment may require a license, e.g.,
  - Radiation hardened or protected from extreme elements
  - High performance computers
- Software and Encryption – may need a license
  - Encryption software with symmetric key length of 64-bits or higher
  - Controlled Software
  - Military support applications
- Export-controlled technical data
  - Best to back-up on a secure system and remove from laptop prior to travel

Encryption ECCN's

The following items are controlled by the EAR (numbers are Export Control Classification Numbers)

- • Laptops, iPhones, Blackberries: 5A992
- • Mass market software (Windows, OS X, Office, Adobe products, Visual Studio): 5D992
- • Open source software (Linux, Apache): 5D002

Data and Information on your device …

- The data on your device could be subject to export controls.
- The results of Fundamental Research you conduct on the UC campus are not export controlled.
- Results of research may be subject to export controls if performed outside the campus.
- Unpublished research data and Proprietary Data from others (such as under Proprietary Rights Agreements/NDA's) may fall outside of Fundamental Research

There may be Exceptions #5

Know which exemptions and exceptions apply

- The requirements for an export license vary according to the general characteristics of the item or technology, the destination country and the intended use of the export.
- Even if an export license is required, a license exception may apply to an export of a laptop, GPS and the loaded software and technical information.
- If a license exception applies, the equipment and technology may be taken abroad without an export license.

Know that ownership matters…

Exceptions vary based on whether an item is personally owned or owned by the University

…as does the dollar value

$2,500 threshold triggers AES Census filings

Could become an issue if a “Temporary Export” extends past one year.

TMP – temporary exports

- Form is good for one year

BAG – baggage - personally owned, NOT University owned

Laptop, equipment must stay under “effective control” for travel to certain countries

SED/AES process

Tools of the Trade Exception

Tools of the trade are commodities and software that are:

(a) Owned by the individual exporter (U.S. principal party in interest) or exporting company.

(b) Accompanying the individual exporter (U.S. principal party in interest), employee, or representative of the exporting company.

(c) Necessary and appropriate and intended for the personal and/or business use of the individual exporter (U.S. principal party in interest), employee, or representative of the company or business.

(d) Not for sale.

(e) Returned to the United States no later than 1 year from the date of export.

Is there an exemption from the Census' AES process, for Tools of the Trade?

- Yes, as long as you do not need a validated license.

FAQs
http://www.census.gov/foreign-trade/regulations/forms/qna.html#lowvalue

TMP (Tools of Trade) for EAR related exports

- Applies to usual and reasonable kinds/quantities of tools (commodities/software) for use by exporter.
- Must remain under effective control exporter or exporter's employee (physical possession, locked in safe, guarded).
- Must accompany exporter when traveling or be shipped within one month before departure or any time after departure, and be returned no later than one year post export.

Does not apply to:

- Satellite or space-related equipment, components, or software
- Exports related to nuclear activities except for a limited number of countries
- Technology associated with high-level encryption
- Travel to Iran, Syria, Cuba, North Korea, or Sudan
- Anything regulated by the Department of State's International Traffic in Arms Regulations (ITAR)

Fundamental Research Exclusion

Basic or applied research in science and engineering at an accredited institution of higher learning in the U.S.

The resulting information is ordinarily published and shared broadly in the scientific community

Fundamental Research Exclusion

- However, the FRE does not apply if the situation involves:

Shipping controlled items to a sanctioned country and/or restricted person

  - An export control license may be necessary

Pre-Travel Advisory Checks:

US State Department publishes International Travel advisories

http://travel.state.gov/travel/cis_pa_tw/cis_pa_tw_1168.html

UC Risk Services - iJet Registration

Additional information about international encryption controls can be found at the following websites:

http://rechten.uvt.nl/koops/cryptolaw/index.htm

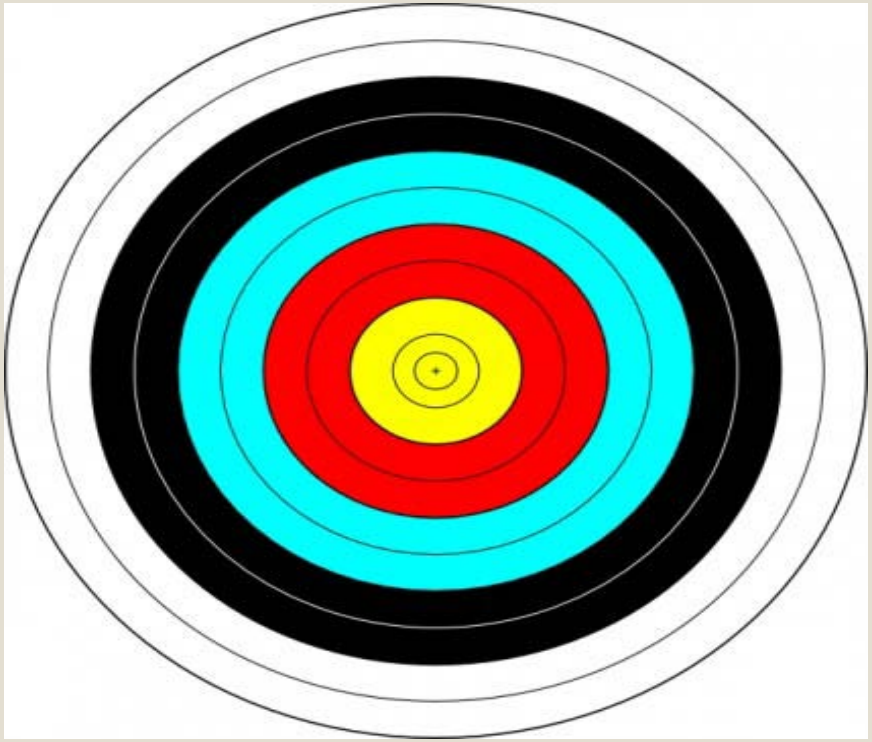
http://www.wassenaar.org/introduction/index.html

Foreign Surveillance

4

YOUR Electronics…

May be vulnerable to Surveillance



The New York Times — Business Day Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SP

Traveling Light in a Time of Digital Thievery

Published: February 10, 2012

(Page 2 of 2)

Both China and Russia prohibit travelers from entering the country with encrypted devices unless they have government permission. When officials from those countries visit the United States, they take extra precautions to prevent the hacking of their portable devices, according to security experts.

Readers' Comments

Readers shared their thoughts on this article.

Read All Comments (113) »

Now, United States companies, government agencies and organizations are doing the same by imposing do-not-carry rules. Representative Mike Rogers, the Michigan Republican who is chairman of the House Intelligence Committee, said its members could bring only "clean" devices to China and were forbidden from connecting to the government's network while abroad. As f said he traveled "electronically naked."

At the State Department, employees get specific instruction on how to secu in Russia and China, and are briefed annually on general principles of secu Brookings Institution. Mr. Lieberthal advises companies that do business in

Best Practices for Data Privacy... *#3*

Might **NOT** work for Export Controlled Data!

Follow Best Practices! # 2

- Exercise reasonable care when hand-carrying a laptop computer to a foreign country
- The laptop:
  - MUST remain in reasonable control of the person(s) responsible for it at all times
  - MUST not be used by anyone in the foreign country
  - MUST not be left behind (upon your return), given away, or out of the US more than 1 year.
- Consider taking a minimal “Wiped” device

Executive Best Practices may include....

1. Clean devices be provided (fresh install – or at least completely wiped of all existing accounts/passwords, email, documents, etc.
2. Set up a temporary email account for each trip and connect that email account to the devices.
3. Intermediary role to filter regular email and send – only as necessary – to the temporary email account.
4. Avoid accessing regular email account(s) from these devices while travelling in certain countries – using only the temporary account.
5. On return ....
    - the devices should be wiped and reconfigured before being redeployed
    - the temporary email account should be closed and deleted.

Before Traveling with Your Laptop

- Consider backing up your data and leave a copy of your files in a safe and secure location such as your office or a departmental shared drive. Don't carry the only copy of data you can't afford to lose.
- Don't carry data you don't want others to see: medical records, data files from your research, financial information, photos, etc.
- Have a "Plan B" if there is data you will need when you reach your destination.
- Password-protect, encrypt (if allowed) or remove all student, personal, and proprietary information stored on your laptop.
- Ensure that your operating system has a strong password or passphrase when it boots up.
- Turn off file-sharing and print-sharing.
- Make sure your system's security patches are up to date and your firewall is turned on.
- Ensure that anti-virus, anti-spyware, and personal firewall software is installed on your laptop.
- Use secure VPN for secure remote access
- Consider purchasing a tracking application for your laptop in case it is lost or stolen.

Steps to Review

Classify the technology or goods involved (ITAR, EAR, OFAC, other?)

Determine if license is needed for the technology/end user/end use

Determine if license exception is available

Document the use of the exception

Steps to Review

If you must travel to one of the five embargoed countries, you may be able to obtain the appropriate export license, but the process can take, on average, a ninety days for review.

The Department of Commerce's Bureau of Industry and Security and the Office of Foreign Assets Control (OFAC) within Dept. of Treasury accept applications for licenses to export encryption products and technologies.

Reality Check

Exporting is a privilege—not a right

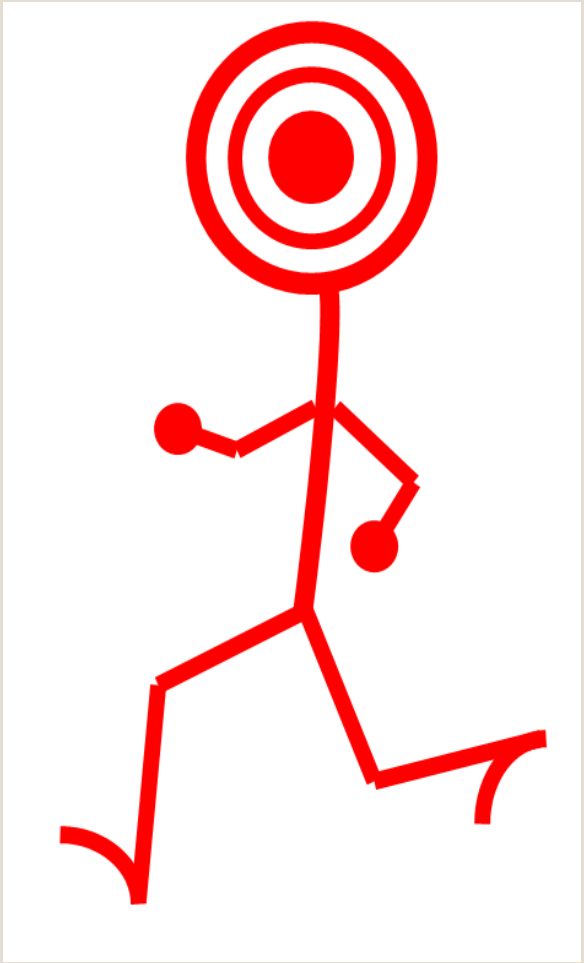
Every situation is unique

Ignorance is not a defense

Seek expert advices BEFORE you Travel!

Stay informed

- Export Control Reform initiative
  Export.gov/ecr
- Current Events



#1

WHO Can You Call With Questions?

Campus Contacts

- LBNL Nancy M Ware NMWare@lbl.gov
- UARC Nasa Ames: Scott Fong scott.fong@uarc.ucsc.edu
- UCB Patrick Schlesinger pschlesinger@berkeley.edu
- UCD Craig Allison ccallison@ucdavis.edu
- UCI Marci Copeland marci.copeland@rgs.uci.edu
- UCLA: Claudia Modlin cmodlin@research.ucla.edu
- UCM Deb Motton dmotton@ucmerced.edu
- UCR Charles Greer, Jr charles.greer@ucr.edu
- UCSB 'Bruce G. Hanley Hanley@research.ucsb.edu
- UCSC Rachel Sievert rsievert@ucsc.edu
- UCSD Brittany Whiting brwhiting@ucsd.edu
- UCSF Eric Mah Eric.Mah@ucsf.edu
- UCOP Brian M. Warshawsky brian.warshawsky@ucop.edu

Useful Links

- http://www.wassenaar.org - Wassenaar Arrangement
- http://www.wassenaar.org/controllists/index.html - Wassenaar Arrangement Control Lists (see Category 5-Part 2, Information Security and Note 3, Cryptography Note)
- http://www.bis.doc.gov/encryption/lechart1.htm - Encryption License Exemption Chart (view the BAG category)
- http://www.bis.doc.gov/encryption/740supp1.pdf - Country Groups lists as viewed by the US Government
- http://www.gpo.gov/bis/ear/ear_data.html - Export Administration Regulations Database (see part 740, License Exemptions, then 740.14 BAGGAGE, (BAG))

Who are we?

- Office of Audit Services, which pre-existed, was combined with the new Regental office of Ethics and Compliance in October, 2007
  - Regental resolution and approval of Ethics and Compliance Program and Structure in July, 2008
- Provides structure of accountability and transparency around compliance and audit
  - Facilitates system-wide ethics, compliance and audit
  - Provides assurance to the President and the Regents that mechanisms are in place to appropriately manage business controls and minimize compliance and audit related risks

Questions?

Brian Mitchell Warshawsky
Brian.warshawsky@ucop.edu
Ethics Compliance and Audit Services
(510)987-0413

Additional Notes

“Every day more than a million people cross American borders, from the physical borders with Mexico and Canada to functional borders at airports such as Los Angeles (LAX), Honolulu (HNL), New York (JFK, LGA), and Chicago (ORD, MDW). As denizens of a digital world, they carry with them laptop computers, iPhones, iPads, iPods, Kindles, Nooks, Surfaces, tablets, Blackberries, cell phones, digital cameras, and more. These devices often contain private and sensitive information ranging from personal, financial, and medical data to corporate trade secrets."

-UNITED STATES V. COTTERMAN

(US CT OF APP NINTH CIR en banc opinion filed March 8, 2013)

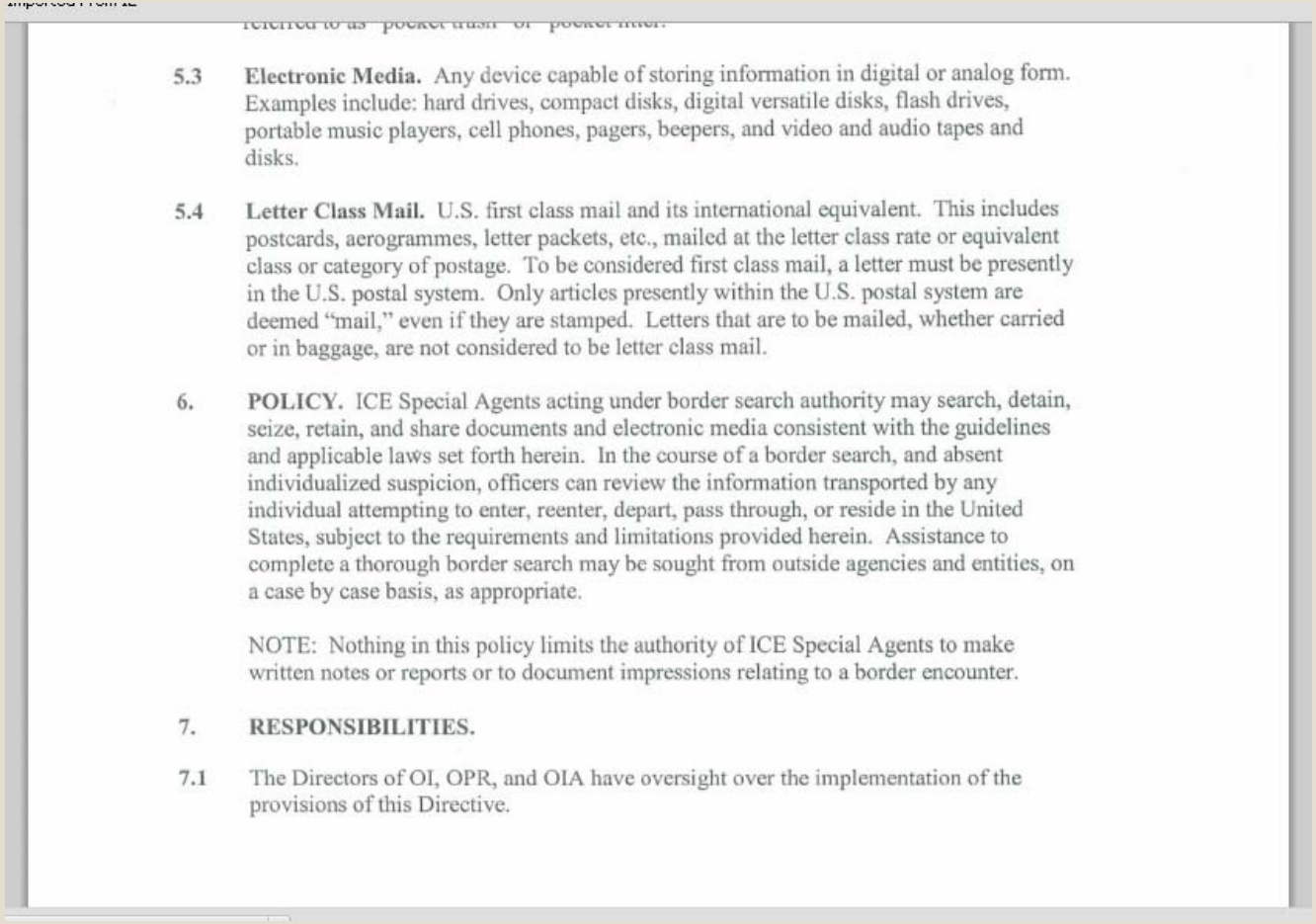
Additional Notes

“The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. That is no longer the case. Electronic devices are capable of storing warehouses full of information. The average 400-gigabyte laptop hard drive can store over 200 million pages -- the equivalent of five floors of a typical academic library. Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage.

-UNITED STATES V. COTTERMAN

(US CT OF APP NINTH CIR en banc opinion filed March 8, 2013)

ICE Policy



5.3 **Electronic Media.** Any device capable of storing information in digital or analog form. Examples include: hard drives, compact disks, digital versatile disks, flash drives, portable music players, cell phones, pagers, beepers, and video and audio tapes and disks.

5.4 **Letter Class Mail.** U.S. first class mail and its international equivalent. This includes postcards, aerogrammes, letter packets, etc., mailed at the letter class rate or equivalent class or category of postage. To be considered first class mail, a letter must be presently in the U.S. postal system. Only articles presently within the U.S. postal system are deemed "mail," even if they are stamped. Letters that are to be mailed, whether carried or in baggage, are not considered to be letter class mail.

6. **POLICY.** ICE Special Agents acting under border search authority may search, detain, seize, retain, and share documents and electronic media consistent with the guidelines and applicable laws set forth herein. In the course of a border search, and absent individualized suspicion, officers can review the information transported by any individual attempting to enter, reenter, depart, pass through, or reside in the United States, subject to the requirements and limitations provided herein. Assistance to complete a thorough border search may be sought from outside agencies and entities, on a case by case basis, as appropriate.

NOTE: Nothing in this policy limits the authority of ICE Special Agents to make written notes or reports or to document impressions relating to a border encounter.

7. **RESPONSIBILITIES.**

7.1 The Directors of OI, OPR, and OIA have oversight over the implementation of the provisions of this Directive.