Laptop Alert!

Ethics, Compliance and Audit Services

International Travel with Mobile Devices

BRIAN MITCHELL WARSHAWSKY, JD CCEP
Systemwide Export Control Officer
Office of Ethics, Compliance and Audit Services
University of California Office of the President
(510) 987-0413 brian.warshawsky@ucop.edu

White House Report:

"Targeting of US Travelers Overseas"

"…via airport searches, hotel room incursions, computer/device accessing, telephone monitoring, personal interchange and the like, these are attempts to gain access to protected information through the presence of cleared contractor employees traveling abroad as a result of invitations, and/or payment to attend seminars, providing training, deliver speeches, and the like."

www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf

In This Issue:

Stopped at the U.S. Border: Steve Liu Case

Steve Liu, an engineer returning to the US from China, travelled with his personal laptop containing files from work at a government contractor. Prosecutors say he transported the files, which included information on the performance and design of sensitive defense technology. The laptop was inspected at Newark Liberty International Airport in November 2010 and Liu was convicted in September 2012 and received a prison sentence of 70 months.

Liu's lawyer, James Tunick, said that Liu had made "a terrible mistake in having these files on his computer and going to China."

http://www.justice.gov/usao/nj/Press/files/Liu,%20Sixing%20Sentencing%20News%20Release.html

http://www.news.net/article/212210/?

Overseas Border Inspections:

The FBI lowered their Time Away Warning from 2 minutes to 90 seconds. At a foreign airport or border, If your device is selected for a momentary out-of-sight inspection lasting longer than 90 seconds, it has been compromised.

New policy at some US companies: If an employee's device was inspected at the Chinese border, it is prohibited from connecting into that company's network. "Ever."

http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?pagewanted=all

Tips and Best Practices!

Travel only with a "clean" device "wiped" upon return to the US.

During private meetings turn device off and remove battery.

Disable Bluetooth, WiFi, print/file sharing. Switch off mic/camera.

90 seconds out of sight with foreign customs and assume it is compromised.

Connect online ONLY through secure encrypted channels.

Avoid typing PASSWORD; Paste from secure file/USB drive.

Screen names of foreign contacts.

Know WHAT is on your device BEFORE you travel. Information and data may carry restrictions.

Encrypted information may still require an export license.

Opening email attachments overseas may be an export.