UNIVERSITY of CALIFORNIA

Quarterly Security Bulletin

Volume 2, Issue 2

Summer 2013

A Message from the UC Research Security Office

For some of you that may not be aware, effective May 1, 2013, I have assumed the role as the University's Facility Security Officer, succeeding Ron Nelson. Any questions you may have regarding your security clearance and other security related matters, please contact me. I look forward to continuing to support each and every one of you.

My hope for this newsletter is to accomplish two important things: enhance your security consciousness and make you aware of security clearance policy developments.

Most University clearance holders are not custodians of classified documents, and unlike custodians are not constantly reminded of their security obligations. Nevertheless as a clearance holder you need to keep security clearly in mind. This newsletter contains stories and articles we hope will help you make security a priority in your life.

As you are aware, obtaining and maintaining a security clearance is an intrusive and complex process. I want to keep you informed of policy developments as I learn of them. This may not necessarily make new requirements pleasant or easier. However, it may result in avoiding any surprises, and may make compliance less stressful for you.

You may also visit us on the Web. There you can find detailed information regarding your security clearance such as reporting requirements, information on foreign travel, and even view our briefings and past newsletters.

Visit us at:
http://www.ucop.edu/laboratory-management/security/index.html

Brandi Marotta
Facility Security Officer

Issue Highlights

2 Classified Information in the Public Domain

3 Hacking and Attacking…are you safe?

5 Keeping Safe on Foreign Travel

7 Recent Articles in the News

9 Security Education Challenge

Updates Regarding your Security Clearance

Revised Instructions for Completing Question 21: The Director of National Intelligence (DNI), in his role as Security Executive Agent, issued a memo dated April 12, 2013, requiring executive branch departments and agencies to inform all individuals completing the Standard Form 86 that the instructions for Question 21 have been modified to advise victims of sexual assault who have received mental health counseling strictly related to the sexual assault to respond "No" to this question. Further, the memo indicates that OPM will modify the instructions to Question 21 in the e-QIP system as follows: "Please respond to this question with the following additional instruction; victims of sexual assault who have consulted with a health care professional regarding an emotional or mental health condition during this period strictly in relation to the sexual assault are instructed to answer No."

SF-86 News: A new version of the SF-86, Questionnaire for National Security Positions, is now being utilized. Some of the changes include detailed branch questions for questions answered "yes." This may increase the size of the SF-86; however, it should reduce the comments section. The Office of Personnel Management has also developed a Fair Credit Release form, which will accompany the other e-QIP signature pages. This will replace the Department of Energy (DOE) Fair Credit form you have signed in the past. Furthermore, you are now to use a "Click to Sign" function for the Certification (CER) and Fair Credit Release (FCR). This eliminates the need for separate attachments for CER and FCR.

SF-86, QNSP Copies: Need a copy of your SF-86, Questionnaire for National Security Positions (QNSP)? Please contact our office for assistance in sending your request to the DOE Service Center.

The QNSP copy, if requested, will either be faxed or be mailed due to the use of Personal Identifying Information.

Classified Information in the Public Domain

Information that is considered classified by the US government, may, on occasion, appear in the public domain, in print, or in broadcast media reports. However, the appearance of such information in open sources does not automatically make it unclassified.

In accordance with DOE's "No Comment Policy", as a cleared employee, you cannot comment on the accuracy, technical merit, or classification status of any classified information that appears in the public domain. This includes articles in newspapers or magazines, books, speeches, etc.

If you are not sure about the classification status, you should avoid comment. Also, remember that just because classified information has appeared in the public domain does not mean that the information has been declassified.

Hacking and Attacking…are you safe?

As you know, the World Wide Web is a dangerous place. As soon as you connect, you are vulnerable to an attack. You can put up firewalls and add virus protection, make convoluted 32 character passwords, but you are still susceptible! Hackers are constantly coming up with new tactics, becoming more creative and habitually challenging the United States cyber infrastructure. Surprisingly, one of the most common forms of attack is email hacking. Email hackers are accumulating as much information as they can and find a way to use it against you. Something as simple as knowing the answer to "What high school did you attend?" can lead an email hacker into an intricate weave of stealing your personal information, or even your identity.

So what can you do protect yourself? Below are some key steps to protected your computer, and yourself, from being hacked:

1. Use *"anti-virus software"* and keep it up to date.

Make sure you have anti-virus software on your computer. Anti-virus software is designed to protect you and your computer against known viruses so you do not have to worry. But with new viruses emerging daily, anti-virus programs need regular updates, like annual flu shots, to recognize these new viruses. Be sure to update your anti-virus software regularly. The more often you keep it updated, weekly for example, the better. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to obtain regular updates for your software.

2. Do not open email from unknown sources.

A simple rule of thumb is that if you do not know the person who is sending you an e-mail, be very careful about opening the e-mail and any file attached to it. Should you receive a suspicious e-mail, the best thing to do is to delete the entire message, including any attachments. Even if you do know the person sending you the e-mail, you should exercise caution if the message is unusual and unexpected, particularly if it contains unknown hyperlinks. When in doubt, delete!

3. Use hard to guess passwords.

Passwords will only keep outsiders out if they are difficult to guess! Do not share your password, and do not use the same password in more than one place. If someone should happen to guess one of your passwords, you do not want them to be able to use it in other places. The golden rules of passwords are:

- A password should have a minimum of 8 characters, be as meaningless as possible, and use uppercase letters, lowercase letters and numbers, e.g., xk28LP97.
- Change passwords regularly, at least every 90 days.
- Do not give out your password to anyone!

Continued on next page

Common SF-86 Form Errors

Q What attachments are required when submitting a form in e-QIP?

A All release pages must be attached. This includes the release for Fair Credit, Authorization, Certification, and Medical, if applicable.

Q What are common errors with the release pages?

A The release pages must be signed using your proper name at birth and all handwritten information must be completed (Date of Signature, DOB, and SSN).

Q Are complete mailing addresses required on the questionnaire?

A Yes, please ensure you have entered complete mailing addresses for education, employment, personal references, court actions, etc. P.O. Boxes will NOT be accepted.

Q What if I go by different names, how should it appear on my questionnaire?

A The name provided on the SF-86 and signed on the release pages must be the LEGAL name that is currently used and they must match. For example, if an individual has married, but has not legally changed their last name, the maiden name must be shown.

Hacking and Attacking…Cont.

4. Regularly download security protection update "*patches*."

Most major software companies today have to release updates and patches to their software every so often. Sometimes bugs are discovered in a program that may allow a malicious person to attack your computer. When these bugs are discovered, the software companies, or vendors, create patches that they post on their web sites. You need to be sure you download and install the patches. Check your software vendors' web sites on a regular basis for new security patches or use the new automated patching features that some companies offer. If you don't have the time to do the work yourself, download and install a utility program to do it for you. There are available software programs that can perform this task for you.

The FBI Cyber Secutiy Division website is a great resource to utlize. They provide information on the lastest internet scams, and provide tools on how to protect your computer. Visit them at : http://www.fbi.gov/scams-safety.

You may also submit a report to the FBI Internet Crime Complaint Center if you believe you recived an email that is a scam. For more information visit : http://www.ic3.gov/complaint/default.aspx

Keeping Safe On Foreign Travel: Know the Common Methods and Responses

Reporting all foreign travel is the norm for those of us who possess a security clearance. While the Department of Energy mandates travel to a sensitive country or travel using DOE funds **have to be reported at least 45 days before departure**, best practice is to report *any* travel outside of the country. As a cleared person, **you are a target**. You have access to useful information that many others desire and when traveling abroad the risk for compromise significantly increases.

When planning a trip to another country, for business or pleasure, you should always talk to the UC Research Security Office prior to your trip. We will provide you with the latest information regarding any hazardous conditions, any known security concerns regarding the areas where you will be traveling and general information on security risks during foreign travel. Another wonderful tool to use when planning a trip is the State Department website: http://www.state.gov/travel/. This site provides pertinent and updated country specific threats, as well as many other useful bits of information. Before setting out on your excursion it is a good idea to sign up for the Smart Traveler Enrollment Program to receive updates on Travel Warnings, Travel Alerts and other information for the particular country you are visiting. Visit https://step.state.gov/step/ for more information regarding this program or to sign up.

In recent publications, the State Department has listed several methods of intelligence gathering that may be used against you when traveling overseas. These methods include:

Assessment: Friendly discussion with local contacts who assess whether you have information of value and seek to identify any personal attitudes, beliefs, problems or needs that could be exploitable.

Elicitation: A ploy whereby seemingly normal conversation is contrived to extract intelligence information of value.

Examples are:

- **Eavesdropping:** Listening to other peoples' conversations to gather information. Frequently done in social environments where attendees feel comfortable and secure and, therefore, are more likely to talk about themselves or their work.

- **Technical Eavesdropping:** Use of audio and visual devices, usually concealed.

- **"Bag Operations":** Surreptitious entry into someone's hotel room to steal, photograph, or photocopy documents; steal or copy magnetic media; or download from laptop computers.

- **Surveillance:** Following you to determine your contacts and activities.

Continued on next page

Keeping Safe On Foreign Travel…Cont.

- **Threat of Information:** Stealing documents, briefcases, laptop computers or sensitive equipment.

- **Intercepting Electronic Communications:** Telephones, fax, telex, and computers can all be monitored electronically.

So, how do you keep yourself and your organizations information safe? Common sense and basic counterintelligence (CI) awareness is the key! Remembering these easy steps can reduce the risk of being a target so your trip can be successful, whether for business or pleasure:

- Arrange a pre-travel briefing from the UC Research Security Office and visit recommended State Department websites to increase your awareness. Know emergency numbers for the U.S. embassy and how to get help if needed!

- Maintain physical control of all documents or equipment at all times. Do not leave items that would be of value to a foreign intelligence service unattended in hotel rooms or stored in hotel safes.

- Limit discussions—hotel rooms or other public places are rarely suitable to discuss information that could be considered sensitive (business or personal).

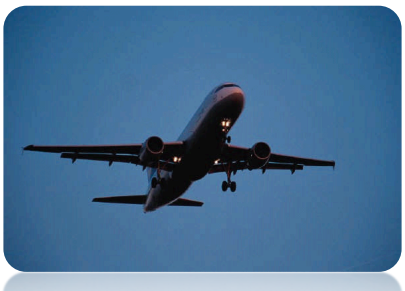
- Do not use computer or facsimile equipment at foreign hotels or business centers for sensitive matters.

- Ignore or deflect intrusive inquiries or conversation about business or personal matters.

- Keep unwanted material until it can be disposed of securely. Burn or shred paper. Keep your laptop computer as carry-on baggage—never check it with other luggage and, if possible, remove or control storage media.

- While on travel try to blend in and vary your routes—practice Operations Security (OPSEC)!

- Check in upon return and report any CI incident to the relevant U.S. Government agency and/or the UC Research Security Office.



Recent Articles in the News

Why the Professor Went to Prison

"After lunch in his cell in the federal prison in Ashland, Ky., John Reece Roth noticed something unusual. Tiny red ants were swarming across his floor, feasting on candy bar scraps. Knowing that ants establish a trail to and from their food, Roth devised a trap: a Möbius strip with an on-ramp but no off-ramp. Ants carrying their prize home would climb onto the strip—a sheet of paper half twisted to have only one side and one edge—and be corralled. Fortunately for them, Roth couldn't test his contrivance properly because the Scotch tape needed to secure it is contraband at Ashland.

"I still have some inventing ability," says Roth, in a resonant voice that once filled lecture halls at the University of Tennessee in Knoxville. Round-faced and bespectacled, he exudes poise and self-assurance, even wearing prison khakis and sneakers and leaning on a four-footed cane. Roth, an emeritus professor of electrical engineering, taught and researched at Tennessee for nearly 30 years. A former scientist at NASA, he holds 11 patents and has testified before Congress on nuclear fusion.

He's also the only university professor or administrator ever prosecuted for violating the Arms Export Control Act (AECA). Convicted in federal district court in Knoxville in 2008 of using graduate students from China and Iran on U.S. Air Force research that was off-limits to foreigners, and taking a laptop with restricted files to China, he exhausted his appeals up to the Supreme Court, which declined last year to hear the case. He began serving a four-year prison sentence in January".

See the full article at:
http://www.businessweek.com/printer/articles/79924-why-the-professor-went-to-prison/

Spain Arrests 2 Over Suspected Iran Nuclear Export

"Spanish police have arrested two people and seized equipment made by a Spanish company that was to be illegally shipped to Iran for use in its nuclear program, officials said Friday.

Police officers stopped a tractor trailer at a highway toll booth in the northern town of Durango on Wednesday and after an inspection arrested the two people and seized the cargo, an Interior Ministry statement said. It said the police "dismantled a ring trafficking material for the development of the Iranian nuclear program."

The seized objects included 44 valves made of an alloy "containing more than 25 percent nickel and 20 percent chromium by weight, which ... makes them particularly suitable for use in the nuclear industry," the ministry said."

See the full article at:
http://news.yahoo.com/spain-arrests-2-over-suspected-iran-nuclear-export-144449077.html;_ylt=Agtt2c5zgNkvMW9EgAYWDp.bCMZ_;_ylu=X3oDMTVxdDUyYTZxBGNjb2RlA2dtcHRvcDEwMDBwb29sd2lraXVwcmVzdARtaXQDQXJ0aWNsZSBNaXhlZCBMaXN0IE5ld3MgZm9yIFlvdSB3aXRoIE1vcmUgTGluawRwa

Recent Articles in the News…Cont.

Soldier Receives 16-Year Sentence for Attempted Espionage

"A 22-year-old military police officer in Alaska has been sentenced to a 16-year jail term in connection with his efforts to sell classified documents to a person he believed was a Russian intelligence officer.

In 2011, William Millay was stationed at Joint Base Elmendorf-Richardson near Anchorage when he began to talk to—and solicit help from—other military members regarding selling classified national defense information to the Russians.

"This case really drives home the point that the insider threat is alive and well," said Special Agent Sam Johnson, who supervises a national security squad in our Anchorage Division. "That's why counterintelligence investigations continue to be a very high priority for the FBI."

Millay, who joined the Army in 2007 and had served a combat tour in Iraq, was known to have harsh and sometimes radical views of the military and the U.S. government—the white supremacist tattoos on his body likely reflect his ideology. But his attempt at spying had nothing to do with ideology or politics, Johnson said. Instead, he was motivated by greed".

See the full article at:
http://www.fbi.gov/news/stories/2013/april/soldier-receives-16-year-sentence-for-attempted-espionage/soldier-receives-16-year-sentence-for-attempted-espionage

Company Admitted To Illegally Sending US Military Technology To China

"United Technologies Corp on Thursday admitted selling China software that helped Beijing develop its first modern military attack helicopter, one of hundreds of export control violations over nearly two decades.

At a federal court hearing in Bridgeport, Connecticut, United Technologies and its two subsidiaries, Pratt & Whitney Canada and Hamilton Sundstrand Corp, agreed to pay more than $75 million to the U.S. government to settle criminal and administrative charges related to the violations.

As part of the settlement, Pratt & Whitney Canada pleaded guilty to two federal criminal charges - violating a U.S. export control law and making false statements.

Federal prosecutors said the company knew that its export of modified software to China would allow Beijing to test and develop its new military helicopter, called the Z-10, using 10 engines that had been legally exported as commercial items".

See the full article at:
http://www.businessinsider.com/united-technologies-broke-military-embargo-2012-6

Security Education Challenge - the FBI at Hanford

The Federal Bureau of Investigation (FBI) established an office in Richland Village in the 1940s. The FBI had no criminal investigative jurisdiction at the Hanford Site. This duty was the responsibility of Benton County. Nor did the FBI maintain any security duties at the Hanford Site. However, since the Hanford Site was a federal project, the FBI received security clearances allowing them access to the entire Hanford Site and its buildings. The FBI had three main functions at the Hanford Site:

- Investigate federal crimes against the government, such as theft and fraud
- Investigate employee backgrounds for security clearances
- Investigate violations of the Atomic Energy Act, such as theft of classified materials or trespass in classified areas.

Several permanently assigned agents maintained the office until 1961, when only one agent was permanently assigned. Supplemental agents were assigned during times of increased investigations. During the mid-1940s, normally 15-20 agents were present. This office was part of the Washington State Resident Agency of the FBI and presumably was initially established to support the Hanford Site. However, the Richland office eventually was assigned to also cover all the southwest counties of the state in cases of violations of federal criminal statutes.

The FBI focused on investigating serious crimes. One unusual and unsolved case occurring during the early-mid Cold War era involved the disappearance of twelve copies of the same classified document over a weekend. The courier, who was supposed to deliver the registered documents from the 300 Area to the Federal Building on a Friday afternoon, never showed up. It turned out he was killed in an auto accident the next day in Idaho. The accident scene was searched, but the documents were never recovered. On another occasion, an employee ending employment at the Hanford Site decided to take a souvenir with him when he moved. He took a fuel element. When this was discovered, the FBI tracked down the individual and recovered the souvenir.

Source: History of the Hanford Site 1943-1990.

Take the Security Ed Challenge!

Of the list below, what is the reward offered by the Federal Government for the information leading to the arrest of an individual who steals, introduces, or attempts to export Special Nuclear Materials?

A. $20,000 B. $100,000 C. $500,000 D. $1,000,000

Answer C. $500,000. Any person who furnishes original information to the United States - leading to the finding or other acquisition of special nuclear material or attempted acquisition, or import or attempted import, or export or attempted export shall be rewarded by the payment of an amount not to exceed $500,000. Title 50.