A Message from the UC Research Security Office

This is our first quarterly security newsletter for 2013! We hope this newsletter will 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. We want to keep you informed of policy developments as we learn of them. This may not necessarily make new requirements pleasant or easier. However, it would 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:

Ronald Nelson
Research Facility Security Officer

Brandi Marotta
Assistant Research Facility Security Officer

Issue Highlights

2 DOE Cyber Security Incident
4 Income Taxes and your clearance
5 What do our cars say about us?
6 Travel Tips
7 DHS Active Shooter Information
8 Recent Articles in the news
DOE Cyber Security Incident

From DOE Office of the Chief Information Officer:

The Department of Energy (DOE) has confirmed a recent cyber incident that occurred in mid-January 2013 which targeted the Headquarters’ network and resulted in the unauthorized disclosure of employee and contractor Personally Identifiable Information (PII).

1. How did the possible disclosure of personally identifiable information happen?

Department of Energy networks and employee and contractor information hosted on these networks are protected in accordance with federal laws and Department of Energy policies. We do know that this incident was a sophisticated attack that appears to have originated from overseas and is therefore being investigated as a national security issue, although no classified networks or information were involved. We are working with interagency partners on actions that can be taken against those responsible and to reduce the likelihood of another successful attack.

The Department’s Cybersecurity Team identified and stopped this malicious attack while it was in progress, preventing further damage. The Cybersecurity Team’s quick response enabled robust analysis that will help the Department understand how this attack happened and reduce the likelihood of these events occurring again. At this time, it appears no encrypted documents or information were obtained by the perpetrators.

2. Who may be affected?

As part of the investigation, the Department is determining which employees’ and contractors’ Personally Identifiable Information (PII) was affected. The files containing PII made up less than 1 percent of the total number of files known to be compromised. The Department has identified approximately 1,500 individuals whose name and social security number was potentially affected by this criminal attack.

The Department is notifying these individuals and offering assistance on steps they can take to protect themselves against potential fraud or identity theft. These employees and contractors will be offered one year of free credit monitoring services.

3. How can I tell if my information was compromised?

DOE employees and contractors who do not receive a personal notice by February 28, 2013 should assume it is highly unlikely their PII was potentially affected. If DOE determines your PII was affected you will be notified, regardless of the date of discovery.

Based on the findings of the Department’s investigation into this incident, we do not believe PII theft was the primary purpose of the attack. However, the Department encourages each affected individual to be extra vigilant and to carefully monitor bank statements, credit card statements, emails and phone calls relating to recent financial transactions. More information on preventing, detecting and recovering from

Continued on next page
Updates regarding your security clearance

**SF-86 News:** A new version of the SF-86, Questionnaire for National Security Positions, is now live. 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.

---

**DOE Cyber Security Incident…Cont.**


4. I haven’t noticed any suspicious activity in my financial statements, but what can I do to protect myself from being victimized by credit card fraud or identity theft?

The Department recommends that individuals closely monitor their financial statements and visit the Federal Trade Commission’s Consumer Information web page at [http://www.consumer.ftc.gov/topics/privacy-identity](http://www.consumer.ftc.gov/topics/privacy-identity) for further information on protecting your privacy and identity.

5. What should I do if I received a notification and I confirm my identity has been stolen?

- File a police report with your local police or the police in the community where the identity theft took place.
- File a complaint with using FTC’s Identity Theft Hotline at 1-877-438-4338, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
- You may also notify the Department of Energy Privacy Office within the Office of the Chief Information Officer. This should not be done instead of contacting your local police and the Federal Trade Commission.

6. How is the Department of Energy responding to this attack?

The Department is implementing a full network remediation plan. The Department continues to work with our interagency partners to take aggressive steps to reduce the likelihood of these events occurring again, including:

- Working with public and private sector partners to further harden our networks against attack;
- Conducting deep network scans to ensure the malware has been removed and cannot be restarted;
- Reviewing cost-effective, technical solutions that enable stronger data protection; and
- Analyzing our holdings of sensitive business and personal information and ensuring we do not create or retain it unnecessarily.
Income Taxes and Your Security Clearance

It’s tax season again, therefore it is appropriate to remind clearance holders that part of keeping your security clearance is to maintain compliance with federal, state and local tax laws.

Guideline F: Finical Considerations, under the Presidential Adjudicative Guidelines of 2005, states that failure to file or pay taxes (including income tax evasion) may be a disqualifier for granting or retaining a security clearance. Inability or unwillingness to satisfy debts, which includes your taxes, may also be a disqualifying condition for granting or continuing a security clearance under Adjudicative Guideline F.

If you have run into problems with the IRS or other tax authority over the amount of taxes owed and paid, but are still in the process of an appeal or are have selected to use a tax payment plan, it is not considered a “failure to pay taxes”. As long as you are litigating the tax amount or are current on the plan, the appeal or agreement with the tax authority demonstrates a good faith effort to comply with the law.

Remember, when you are due for your security reinvestigation, you must report if you have failed to file or pay Federal, state or other taxes when required by law or ordinance. Section 26 on the SF86, Questionnaire for National Security Positions (QNSP) asks, “In the past seven years have you failed to file or pay Federal, state or other taxes when required by law or ordinance?” In addition, liens or delinquencies on Federal debts are also reportable on the QNSP Section 26.

Make sure that if you are required to file a tax return that you do so.

The IRS website can be found at: http://www.irs.gov/

The California State Board of equalization website can be found at: http://boe.ca.gov

Did you know?

We are on the web! You can find information regarding your security clearance such as reporting requirements, foreign travel information, view our briefings and so much more at the click of a button.

Visit us at:

What Do Our Cars Say About Us?

Do you or someone you know:

- Have stickers on your back car window indicating each member of your family?
- Have a “My Child is the Superstar at (fill in school name)” bumper sticker?

These are only a few examples of how we unknowingly give predators, and random people specific, personal information about our family and ourselves. These family decals usually feature stick figures and each is clearly identifiable as a mom, dad, kid(s) and family pet(s). In some cases, these car decals even supply the children’s names, school, sport teams and hobbies.

With simple window stickers you have given an abductor, pedophile, and/or home invader everything they need to know about you, your children, where you live, the name of your kid’s sports team, your pet’s name, and where the kids go to school.

If your car is parked in your driveway or in front of your house, relevant information and your address is available to a potential abductor and any other interested party. These individuals can easily find out the home to which the car is registered by simply running license plate numbers through search sites devoted to this task.

Here’s a possible scenario: Armed with this information, child abductors can pose as ‘family friends’ who are sent to pick up ‘Billy (whose hobby is basketball)’ from XYZ School. Mom and Dad were allegedly in a car accident (yes, the abductor knows the make and model of the car and even the license plate number!) and won’t make it on time to pick up the child.

Family decals are not the only car stickers that could be putting you and your family at risk. Other decals on your car such as “I am a proud Navy/Army/Air Force/Marine wife” provide information that can be used inappropriately.

Again, these are only a few examples of how we give criminals personal information about us, potentially making ourselves, and our families their targets. Practice common sense. Just like we have all been educated on what we should and should not post on social networking sites, remember to follow the same common sense when thinking about placing stickers and decals on your vehicle.
Travel Tips

Foreign travel increases the risk of foreign intelligence targeting. You can be the target of a foreign intelligence or security service at any time and any place; however, the possibility of becoming the target of foreign intelligence activities is greater when you travel overseas. The foreign intelligence services have better access to you, and their actions are not restricted within their own country borders.

In a world where reliance on technology continues to grow, foreign entities have increased the targeting of electronic devices such as laptops, computers, and personal media such as Personal Digital Assistants and cell phones.

Travelers should report theft, unauthorized or attempted access, damage, and evidence of surreptitious entry of their portable electronics.

These effective countermeasures can decrease or prevent the loss of sensitive information:

- If at all possible, leave unnecessary electronic devices at home.
- Use designated “travel laptops” that contain no personal or company information.
- Use temporary e-mail addresses not associated with your company.
- Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return.
- Encrypt data, hard drives, and storage devices whenever possible.
- Use complex passwords.
- Enable login credentials on laptops, cell phones, and other devices.

Flashback:

Security Posters from WWII era

Theses posters were developed by various government entities such as the Unites States Office of War Information.
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.

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.

Active Shooter Information
From the Department of Homeland Security:
The Department of Homeland Security (DHS) aims to enhance preparedness through a “whole community” approach by providing training, products, and resources to a broad range of stakeholders on issues such as active shooter awareness, incident response, and workplace violence. In many cases, there is no pattern or method to the selection of victims by an active shooter, and these situations are by their very nature are unpredictable and evolve quickly. DHS offers free courses, materials, and workshops to better prepare you to deal with an active shooter situation and to raise awareness of behaviors that represent pre-incident indicators and characteristics of active shooters.

The new website provides access to:
Active Shooter: What Can You Do Course
Active Shooter Webinar
Active Shooter Workshop Series
Active Shooter: How to Respond Resource Materials
Options for Consideration Active Shooter Training Video
U.S. Secret Service (USSS) Active Shooter Related Research

Access to the new website can be obtained at:
http://www.dhs.gov/active-shooter-preparedness
Recent Articles in the News

Ex-scientist at Bridgestone in Akron indicted in trade-secrets case

A former research scientist at Bridgestone Americas Center for Research and Technology in Akron has been charged again in a trade-secrets case.

A grand jury returned a 15-count indictment Tuesday against Xiao-rong Wang, 50, of Hudson, after attempts to work out a plea deal fell through. He is charged with stealing trade secrets and lying to FBI agents investigating the alleged theft.

Federal prosecutors, in announcing their investigation of Wang in March, said he had burned proprietary information from Bridgestone computers onto six CDs in 2010. The FBI said it searched Wang’s house and found CDs with Bridgestone trade secrets. Agents confiscated them and seized Wang’s U.S. passport.

Wang’s attorney, Paul Adamson at Burdon & Merlitti in Akron, said Wang took several CDs when he was terminated from Bridgestone that included a jumble of data, parts of which belonged to Wang, other parts that were not proprietary, and other information that the government contends included Bridgestone trade secrets.

Adamson said the case turns on Wang's intentions -- whether he violated a provision of the Economic Espionage Act that requires that prosecutors establish that Wang meant to use Bridgestone secrets for his economic benefit or someone else’s.

See the full article at:

American Universities Infected by Foreign Spies Detected by FBI

Michigan State University President Lou Anna K. Simon contacted the Central Intelligence Agency in late 2009 with an urgent question.

The school’s campus in Dubai needed a bailout and an unlikely savior had stepped forward: a Dubai-based company that offered to provide money and students.

Simon was tempted. She also worried that the company, which had investors from Iran and wanted to recruit students from there, might be a front for the Iranian government, she said. If so, an agreement could violate federal trade sanctions and invite enemy spies.

The CIA couldn’t confirm that the company wasn’t an arm of Iran’s government. Simon rejected the offer and shut down undergraduate programs in Dubai, at a loss of $3.7 million.

Hearkening back to Cold War anxieties, growing signs of spying on U.S. universities are alarming national
Recent Articles in the News…Cont.

security officials. As schools become more global in their locations and student populations, their culture of openness and international collaboration makes them increasingly vulnerable to theft of research conducted for the government and industry.

“We have intelligence and cases indicating that U.S. universities are indeed a target of foreign intelligence services,” Frank Figliuzzi, Federal Bureau of Investigation assistant director for counterintelligence, said in a February interview in the bureau’s Washington headquarters.

See the full article at:  

Cyber espionage campaign targets energy companies

Hackers using a Remote Access Trojan (RAT) named Mirage have been engaged in a systematic cyber espionage campaign against a Canadian energy company, a large oil firm in the Philippines and several other entities since at least this April, Dell’s SecureWorks Counter Threat Unit says.

The campaign is the second one targeted at oil companies to be discovered by SecureWorks this year. In February, researchers at the firm discovered attackers using remote access tools similar to Mirage to target several oil companies in Vietnam. That campaign also targeted government agencies in several countries, an embassy, a nuclear safety agency and multiple business groups, according to SecureWorks.

The domains for three of the command and control (C&C) servers used to control Mirage and for several of the C&C servers used in the February campaign, appear to belong to the same individual or group of individuals, SecureWorks said.

See the full article at:  
http://www.computerworld.com/s/article/9231596/Cyber_espionage_campaign_targets_energy_companies

If you would like to see us address a particular topic, process, or guideline in a future newsletter, please submit your request to the Research Security office at Brandi.Marotta@ucop.edu