U.S. Department of Energy

Security and YOU

The Office of Health, Safety and Security

Any comments, questions, or suggestions on this newsletter are welcome. Please contact Paul Ruehs, Security Awareness Program Manager, Office of Headquarters Security Operations

Phone: 301-903-7189
E-mail: Paul.Ruehs@hq.doe.gov

Protecting Your Privacy Information

Failure to protect *Personally Identifiable Information* (PII) can harm you. If your personal information falls into the wrong hands, your financial credit can be damaged, your bank account looted, and you may even find that you are the target of identity theft or worse.

So, what exactly is PII? PII consists of information pertaining to an individual's education, financial information, medical history, criminal or employment background, or information which can be used to distinguish or trace their identity, such as their name associated with their social security number, date and place of birth, mother's maiden name, biometric records, etc.

Examples of PII include but are not limited to:

Name, such as full name, maiden name, mother's maiden name, or alias, personal identification number, such as a social security number, passport number, driver's license number, taxpayer identification number, or financial account or credit card number, and personal characteristics, including photographic image (especially of the face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry).

Discarding PII in trash cans or recycling bins poses a serious problem. For example, the recycle bins at DOE Headquarters (HQ) are not secure. Unfortunately, PII information is periodically found in trash bins, waste baskets and recycle bins at DOE HQ. The recycled paper trash at DOE HQ is picked up by a contractor who was awarded the contract because he offered the lowest bid to complete the work. There is no mechanism in place to prevent the contractor from selling the recycled paper trash to someone else. Boat loads of recycled paper trash leave the United States and go to foreign countries. The trash receptacles at your home are even less protected. Sensitive PII materials placed in garbage cans at private residences provide a wealth of data about the owner and are a magnet for those wishing to collect PII for nefarious reasons.

Failure to protect PII can result in identity theft or fraudulent use of one's bank account or credit. We need to be diligent in our efforts when disposing of PII. Remember the bad guys are relying on you to provide them information for your loss and their gain. As a rule of thumb, you should carefully look over bills, financial and medical records and anything else that may contain PII before you dispose of it. It is best to destroy PII by shredding. If you don't own a shredder, you may wish to purchase one. While at work, DOE policy requires that documents containing PII must be destroyed by shredding. It should not be put in the recycle bins but rather disposed of by authorized means, i.e. shredding. As an alternative to local shredding, PII waste can be placed in plain brown paper bags and delivered to the Burn Bag Rooms (Forrestal Room GI-007 or Germantown Room R-002). Please remember that PII can never be placed in office recycling or trash containers. When disposing of PII at your home, be sure to destroy it in such a way as to prevent its reconstruction, i.e., burning, tearing, or shredding.

Smartphones and Mobile Devices

Other concerns are cell phones and mobile devices. Personal Smartphones and other types of mobile devices are high on the list of problem devices when it comes to protecting PII. These devices are capable of storing very large amounts of sensitive data. What some tend to forget is that when you trade in your phone or sell it to the highest bidder in order to save a buck, you may be putting yourself at risk for identity theft or worse. Figures show that there are large amounts of information still left on these devices. A recent study found that if you took 10 phones from recycling companies, the probability is that 60 percent of those still contain data. What kind of data? What don't you do on your mobile device? Some experts say they would rather have someone's mobile device than their PC or their laptop. Data such as information found on social media sites, pictures, comments, political views and details of the individual's job, not to mention personal information or PII, can also be found on mobile devices. We use our mobile device for just about everything.

The best way to prevent identity theft and keep private information private is to get a hammer and smash the smithereens out of that old device (don't forget eye protection) and forgo the 10, 20, or 210 dollars that you could have gotten for a trade-in. Financially, it could save you thousands of dollars and many headaches.

The Dangers of Cyberspace

In the age of rapid communication and personal computers, it is essential to understand the dangers of releasing personal and/or PII data to unknown entities. The Web and social media have created a level of transparency that never before existed in our country. There's no doubt that the Internet has made it much easier to

collect PII through lapses of security on the "net." Cybercriminals armed with PII like e-mail addresses can sell the information on the black market or move forward with highly lucrative phishing or other scams on their own. Phishing is the fastest-growing tactic used by cybercriminals to extract valuable data, since bank and credit card information has become so much harder to get directly. Phishing is popular among cybercriminals because it focuses on the weakest link in any security chain - people. People naturally trust names and information that are familiar and expected, so they fall victim relatively easily to these scams.

Security shortfalls can lead to a profitable market in collecting and reselling personal data. It can also allow a criminal to know your schedule, place of business and where you and your family live. Setting a social media profile to allow anyone, not just friends, to look at postings can make your profile a particularly rich source of information. Be very careful as to what type of personal information you put on the Internet. You should be especially cautious when using social media sites such as Facebook, Twitter, Flickr and YouTube. For example, your safety could be put at risk by geotagged photos - marked with a location - on social media sites. Facebook's new Timeline feature, which creates a map of places geotagged by users, can also be dangerous. So doing allows anyone to know where you are and what you are doing. Keep in mind many smartphones automatically geotag photos with GPS coordinates. In 2007, four US Army helicopters were destroyed in Iraq after geotagged photos were posted on the internet alerting the enemy to the exact location of the aircraft. *Don't put out information that you would not want to share with the world.*

Headquarters Facilities Master Security Plan

Are you familiar with the DOE Headquarters Facilities Master Security Plan or HQFMSP? If not, you should be. Referred to simply as "The Plan," the HQFMSP informs employees of the security procedures in place at DOE HQ. It describes existing DOE security policies and procedures for all HQ facilities and Elements. Additionally, the Master Plan describes the organizations designed to protect the property and national security interests of the HQ complexes in the Washington, D.C. metropolitan area. The Plan does not establish any new security requirements: security requirements are established by various Federal laws and regulations, Executive Orders, and DOE directives. This Plan merely explains how those requirements will be implemented at DOE HQ. It is important that all DOE HQ personnel and visitors have access to the security policies and procedures that affect them on a daily basis. This Plan does not apply to any DOE site or facility outside the Washington, DC area. The Plan can be viewed at:

http://www.hss.doe.gov/hqsecop/hqfmsp/toc.html

Chances are, when it comes to HQ security policy and requirements, you will find the needed information in the Master Plan.

Access to Classified Information

Are you familiar with the term "classified information"? Even if you do not work with, or have access to, classified information, you should know what it means. Classified information is information identified as information determined to require protection against unauthorized disclosure under Executive Order 13526, Classified National Security Information, which is identified as National Security Information or Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954. Access to classified information is granted only to those who possess the appropriate security clearance, sometimes referred to as an "access authorization", and who requires access in the performance of official or contractual duties. The operative word here is "official." Just as the holder of the information is responsible for its protection, he/she is also responsible for releasing/disseminating classified matter appropriately. If you pass classified matter to another individual, you must ensure two things: 1) the recipient has the correct security clearance, and 2) he/she has a need-to-know, i.e., requires this information to do their job - for official business.

If you do not possess a security clearance, you are not authorized to handle classified information. However, should you come across unsecured or improperly protected classified information, you will need to know how to handle it. In the event you find a classified document unprotected, and even though you don't have a security clearance, you must protect the document and/or information until an appropriately cleared security official retrieves it. You should immediately contact one of the following to take possession of the classified matter:

* **Your organizational Headquarters Security Officer (HSO), or a**
* **Protective Force Officer.**

Under no circumstance should you destroy or modify the classified matter.

Be sure to address security concerns and questions to your Headquarters Security Officer (HSO); however, if you would like more information on these or other security related subjects, please call (301) 903-9990.

Emergency Telephone Numbers

Forrestal, Germantown & 955 L'Enfant buildings **dial extension 166**
270 Corporate, Cloverleaf, & 950 L'Enfant buildings **dial 9-911**