

ESH 223 - Cyber Security Education and Awareness

Introduction

The cyber security program at Argonne National Laboratory promotes the safe use of information technology. Argonne plays a key role in America's continued leadership in computing sciences. However, the Laboratory must balance the expansion of computing technology with the need to protect its information infrastructure.

The threat to Argonne's cyber security is real. On an average day, the Laboratory defends against roughly 600,000 attempts to gain access to Laboratory systems. That's about 219 million attacks annually!

These attempts range from automated systems, such as SPAM and network probes, to more concise, targeted attacks against our employees. Unfortunately, even after all of our attempts to defend against these attacks, we still have roughly 10 successful attempts a year.

Because Argonne has distributed computing, cyber security must be a shared responsibility. **Players include Laboratory management, the Cyber Security Program Office, various system administrators and the end users.** This course was developed to help you meet your cyber security responsibilities.

After you complete your annual cyber security refresher, you will be able to:

- Recognize your role in the cyber security program.
- Prevent computer misuse.
- Prevent e-mail viruses and worms from entering your system.
- Identify the importance of backing up your data regularly.
- Recognize the importance of protection of Argonne records.
- Identify critical and sensitive information.
- Identify and prevent phishing and social engineering practices.
- Prevent computer theft.
- Recognize your responsibilities in the cyber security program.
- Report computer incidents properly.
- Recognize the importance of the Argonne National Laboratory Computer User Agreement.

Passwords

Cyber security starts as soon as you log in to your computer. Two of the first key methods of keeping Argonne's computing and networking resources secure are:

- selecting a secure password following DOE guidelines and
- changing your password at least once every six months.

At Argonne, passwords must:

- Consist of at least eight (8) non-blank characters
- Consist of a combination of:
 - Letters (upper and lowercase)
 - Numbers
 - At least one special character in first 7 positions (@#%&*!)

They must NOT:

- Include common words such as 'dog,' 'cat' or 'mom'
- Use numerals in the first or last position

10/12/10

Page 1 of 15

The official version of this training course can be found at,
<https://www.wbt.anl.gov/CourseContent.asp?COURSENO=ESH223>

The paper copy may be obsolete soon after it is printed.

- Be a simple pattern of letters or numbers such as xyz123
- For more information about passwords and guidelines, click [here](#).

Password Rules

You may find it easier to remember your password if you base it on a pass-phrase that is important to you. A pass-phrase can be a set of words taken from a book, song, quotation or anything else that you can always recall. Simply make sure that it meets the requirements for length and combinations of letters (mixed case), special characters and numbers.

Pass-phrase: "Four score and seven years ago, our fathers..."

Password: Fs&7yAoF

Do not keep your password written on paper or embedded in computer files, and do not share your password with or disclose it to anyone else. Unauthorized sharing of passwords can result in disciplinary action up to and including dismissal. **System or network administrators should never ask you for your password. Notify your local Cyber Security Program Representative ([CSPR](#)) of requests for passwords.**

Locking your Workstation

Remember to lock your workstation! Argonne has configuration management to configure computers to automatically lock after 15 minutes of keyboard or mouse inactivity. In order to unlock your workstation, you must enter your password. If you leave your workstation for a short time (e.g. to pick up a printout or go to the restroom), you should manually lock the workstation.

[For detailed instructions on how to lock your workstation, click here.](#)

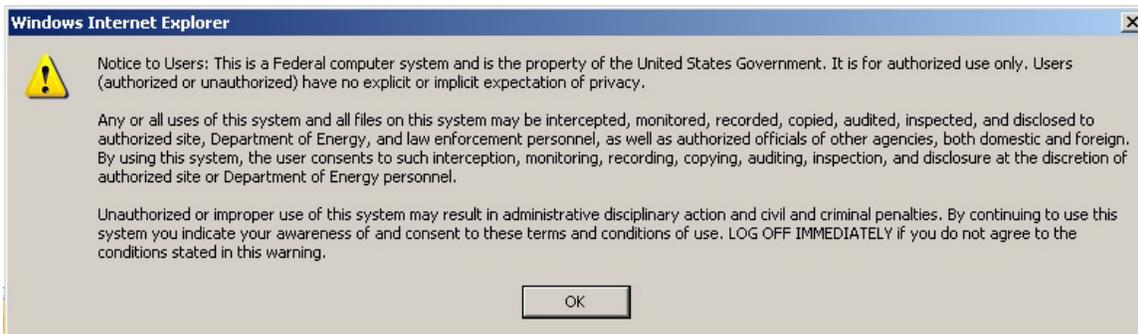
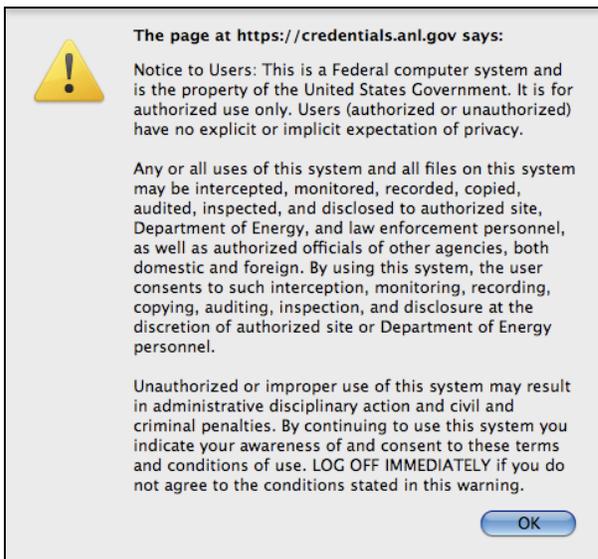
The Lab Monitoring and Warning Banner

The Laboratory provides access to state of the art computing and network resources, including some resources generally unavailable to the public, industry, and academia.

The Laboratory expects end users to use these resources professionally, responsibly and in the best interests of the Laboratory. Argonne monitors usage of its computing and network systems to verify that this expectation is being met and that no abuse of the systems is taking place.

Each time you log in to a computer at Argonne, you should see a banner pop up to inform you about Argonne's monitoring practices. By clicking OK, you give your consent to the kind of monitoring described in the banner. If you do not see this warning banner when you log in, contact your [CSPR](#).

Few Examples of “Warning” Banners



Computer Misuse

Although personal use of Argonne computing resources is allowed, it is not to be abused. Argonne computer users must not engage in activities that are illegal, prohibited by laboratory policy or that are likely to incur incremental costs not related to Argonne’s overall missions.

Examples of prohibited activities include using Laboratory computers to:

- Access inappropriate Internet web sites such as sexually explicit or gambling sites.
- Receive, send, generate or store documents related to a personal business.
- Attack other sites.
- Participate in activities that are illegal or that otherwise may cause disrepute or legal liability for the Laboratory. (See HR Policy [HR-7.4.0.0.1](#))
- Violate software license agreements.

This is not a comprehensive list. Engaging in any of these or similar prohibited activities can result in disciplinary action up to and including dismissal. (See [Argonne Policy ARGPOL-6.11](#))

Scientific Data Records

Recorded information that you create as part of your work at the Laboratory is an Argonne record. Records are created and maintained in many media: digital, paper, tape, film, etc. Records created as part of your job are the property of either the federal government or UChicago Argonne LLC. When you leave Argonne, any original Argonne records that have been in your custody must remain at the Laboratory.

Argonne records must be preserved for periods of time set by the Department of Energy and the National Archives and Records Administration. The length of time a record must be kept depends on its content.

To learn what requirements apply to records in your custody, contact your divisional records coordinator or the Argonne Publications and Records Group.

Click [here](#) to view the retention schedules that apply to Argonne records. Record retention policies have also been established for E-Discovery.

Sensitive Unclassified Information

Information or services that must be specially protected from alteration or disclosure is often known as Sensitive Unclassified Information (SUI). SUI is comprised of the following information that you may be working with at the laboratory. This data may exist in paper OR electronic form:

- Financial risk
- Legal risk
- Privacy act
- Export Controlled Information (ECI)
- Official Use Only (OUO)
- Operations Security (OPSEC)
- Applied Technology
- Unclassified Controlled Nuclear Information (UCNI)
- Essential for day-to-day operation
- Collaborative Research and Development Agreements (CRADA)
- Personal Identifiable Information (PII)

These types of information require additional protection. Argonne SUI is not allowed to be stored on home computers.

Contact your [CSPR](#) and review [ARGPOL-14.1](#) if your work involves critical/sensitive information.

SUI

Desks

Do not leave paper documents or electronic media on your desktop. SUI should never be displayed or exposed to unauthorized persons. It might be appropriate to use locked filing cabinets to store some SUI.

Please contact the [Cyber Security Program Office](#) for more information.

Computers

Laboratory computers store certain sensitive data. Only authorized employees may access sensitive data. SUI is not allowed to be stored on home computers under any circumstances.

Please contact the [Cyber Security Program Office](#) for more information.

Filing Cabinets

To protect the information from alteration or disclosure, you may store certain Sensitive Unclassified Information in **LOCKED** filing cabinets.

Please contact the [Cyber Security Program Office](#) for more information.

Bulletin Boards

Sensitive Unclassified Information should **NEVER be displayed** on bulletin boards or exposed in any other way to unauthorized persons.

Trash Cans or Recycling Bins

SUI should never be discarded in trash cans or recycling bins. Paper documents should be shredded and electronic media containing SUI should be rendered unusable when discarded.

Personal Identifiable Information (PII)

Not all Argonne employees have access to the same types of SUI, but we all have our own PII. Argonne works to protect the PII it collects from its employees to prevent identity theft. You should also take measures to protect your own PII. DOE has defined PII as your first and last name combined with any of the following:

- Social Security Number
- Passport Number
- Credit Card Number
- Clearance Levels
- Bank Numbers
- Biometrics
- Date of Birth
- Place of Birth
- Mother's Maiden Name
- Criminal Record
- Medical Records
- Financial Records
- Educational Transcripts

The Laboratory is required to report any loss of PII to Congress within 45 minutes of the discovery of the loss. **If you feel that the security of your PII may have been compromised, it is imperative that you contact your [CSPR](#) immediately.**

The Laboratory has a PII policy that can be referenced [here](#).

Personal Identifiable Information (PII)

If you think you have Argonne-specific PII stored on your computer or in paper form, contact your CSPR. Your CSPR will make a [Critical Program Infrastructure](#) entry.

Examples of PII include

- Foreign national assignments
- Full school transcripts
- Conference credit card information
- Passport information for travelers

NOT PII

- Pay Grades
- Badge Numbers
- Performance Appraisals

Argonne is not responsible for the protection of PII that is not Argonne specific, such as personal credit card or banking information. Employees are discouraged from storing this type of information on Laboratory computers do so at their own risk.

Information Protection

Most people recognize that their computers store sensitive information that is vital for their daily work and for the operation of the Laboratory. However, many computer users overlook the fact that sensitive data may be exposed as a result of discarding:

10/12/10

Page 5 of 15

The official version of this training course can be found at,
<https://www.wbt.anl.gov/CourseContent.asp?COURSENO=ESH223>

The paper copy may be obsolete soon after it is printed.

- Paper print outs
- Portable media devices such as floppy disks, CD-ROMs, and memory sticks
- Computers

These low-tech exposure risks can be eliminated by following simple strategies:

- Shred sensitive documents; do not simply place them in a recycling container.
- Erase electronic media before destroying it or submit it to CIS's electronic media destruction program. Please contact your [CSPR](#) or the CIS Help Desk at 2-9999 - Option 2 for guidance.
- Deliver unneeded computers and hard disks to your [CSPR](#) for sanitization and disposal. Unneeded computers **must** be sanitized prior to disposal.

Data Awareness Survey

In order for the Laboratory to ensure protection of sensitive data of our customers, employees and the public, it is important that the Cyber Security Office be aware of where such data is at on the Argonne network.

Please fill out the survey at the end of the course, and fax it back to the Argonne Cyber Security Office at (630) 252-9689.

Privacy Act

What is the Privacy Act about?

- The Privacy Act of 1974 (5 U.S.C. 552a) establishes controls over what personal information is collected and maintained by the Executive Branch and how the information is used.
- The Privacy Act grants certain rights to an individual on whom records are maintained, and assigns responsibilities to an agency which maintains the information.
- All DOE employees and contractors are subject to the Privacy Act and must comply with its provisions.

What is the System of Records (SORs)?

Clause H.9 (Privacy Act Records) of the Prime Contract identifies the following SORs for which the Laboratory is responsible for ensuring compliance with the Privacy Act:

- Personnel Medical Records (excepting Contractor employees)
- Personnel Radiation Exposure Records
- Employee and Visitor Access Control Records
- Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites

What shall the employees do?

- Ensure that personal information contained in a System of Records, to which they have access to or are using to conduct official business, is protected to ensure security and confidentiality.
- Ensure that requests for information protected by the Privacy Act are in writing and signed.
- Not disclose personal information except as authorized.
- Report any unauthorized disclosures to your supervisor.

What shall the managers do?

Ensure that all personnel who either have access to a System of Records or who develop/supervise procedures for handling records are aware of their responsibilities for protecting personal information.

What are the penalties for violating the Privacy Act?

- Both criminal and civil penalties are addressed in the Privacy Act for non-compliance.
- The penalty is a misdemeanor criminal charge, and a fine of up to \$5,000 for each offense and/or administrative sanctions. Courts may also award civil penalties.

Social Engineering

Social Engineering (SE) is the practice of obtaining confidential information about a given individual and/or their company through the art of deception, and it usually leads to identity theft. SE risks are always present at home and at the Laboratory. Contact either your local [CSPR](#) or the [CSPO](#) when you receive what you believe to be an SE attempt.

Be aware of suspicious requests in person, over the phone, or through e-mail for information such as:

- User names
- Passwords
- Organization charts
- Installation of software or security patches

Any media (CDs/DVDs, USB drives, memory cards) you receive that you did not specifically request should be treated with great care. Ignore e-mail hoaxes, and do not pass them on.

Check with your [CSPR](#) if you think an e-mail is a hoax, or check a website such as <http://www.snopes.com/computer/>.

Phishing

E-mail is one of the most common platforms for Social Engineering attacks. Approximately 82% of all e-mail received at Argonne is tagged as spam. Most computer users know not to respond to spam e-mail, especially e-mails requesting personal information, since no legitimate organization is going to ask you for personal information via e-mail. But did you know that just by clicking on a link or downloading and opening an attachment from an e-mail, malicious software can be downloaded and installed on your computer without your knowing it?

This is exactly what happens in phishing attacks. **Phishing is an attempt to trick you into giving away personal information or installing malicious software by clicking on a link or opening an attachment in an e-mail.** If this happens at the Laboratory, not only is your personal and professional data at risk for destruction or to be given away, but your computer can be used to infect the machines of your coworkers around the Laboratory.

Normally, the Laboratory firewall stops malicious links and attachments. But a new virus can slip through before the firewall can be updated, creating a window of vulnerability for the whole Laboratory. When this happens, links or attachments can also silently load onto your machine. Once installed, the malware is behind the firewall and can send your personal data out. And now, the malware can use your computer to infect other computers behind the firewall.

One common phishing method is to send you an e-mail that asks you to verify an account or to look into a problem with an account by clicking on a link. If you were to click on the link, you would be taken to a page that looks just like PayPal, for example, but isn't PayPal at all. If you typed your password in, you would be giving your info to the attacker. But worse than that, malware may be silently installed on your computer, putting personal and Laboratory data at risk.

Phishing scams come in all forms. In recent years, federal laboratories have come under increasingly sophisticated cyber security attacks. Many of these attacks come by e-mail, and the

most effective appear to come from sources such as partner institutions, federal agencies or Laboratory management. In order to raise awareness of phishing attacks at the Laboratory, in 2006, the CSPO conducted a social engineering assessment approved by Laboratory management against a small number of Argonne employees.

The assessment worked like this: using a system operated and controlled by the CSPO, an e-mail was sent to 400 Argonne e-mail addresses. The e-mail included information about a recent Argonne Open House and a link that would supposedly take the user to pictures from the event.

=====
From: Argonne Open House [mailto:openhouse@anl.gov]
Sent: Thursday, October 19, 2006 9:38 AM
To: <User>
Subject: Argonne Open House Pictures

<First Name>,

We hope that you enjoyed the ANL Open House. If you missed it, we took the time to take some pictures throughout the day. Click on the link below to browse the online picture gallery.

Click Here -> Pointed to:
<http://www.fireinthehole.org/.anl.gov/UI/login.php?id=83QU6EOc7k>

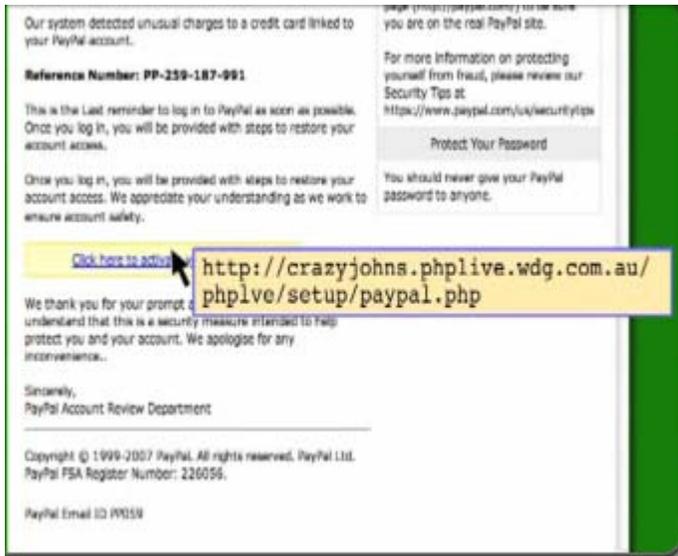
=====
In order to simulate a real phishing attack, the CSPO carefully worked through the process, making every effort to ensure that only public information gathered off of the Argonne web was used in deriving the audience and the topic – information that any malicious user would have access to. The e-mail addresses were harvested from public-facing Argonne websites, and the Open House was chosen as a lure because the event had been covered in newspapers.

If the user clicked the link in the e-mail, he was directed to a website running on the CSPO web server that had the look and feel of the Argonne portal login and requested a username and password. If the user input his username and password, he was directed to a social engineering awareness page that discussed the specifics of this exercise and tips that can be used to aid in detection of real social engineering attempts. The CSPO did not collect any of the usernames or passwords that were supplied.

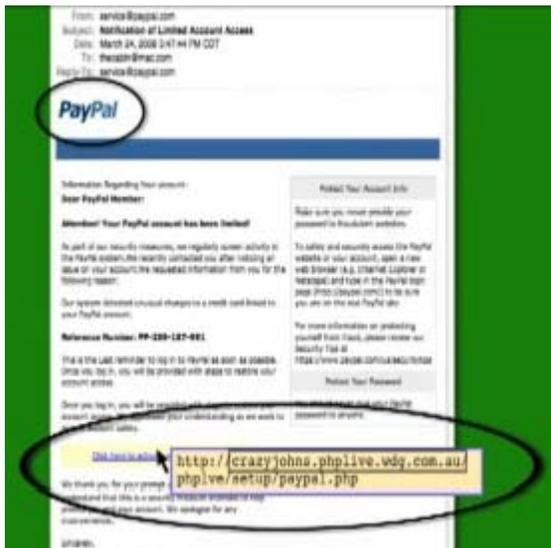
How many users were fooled? The e-mail was sent at 9:38 AM. Within just 5 minutes, 23 users had clicked the link. Of those 23, 17 had entered their username and password.

By 9:43, a user in BIO had reported the e-mail as suspicious. Had this been a real phishing attempt, the CSPO would have put in a block on that URL. By the time the CSPO estimates the blocks would have been put in, 40 users had entered their usernames and passwords.

Within an hour of the e-mail being sent, 100 of the 400 people who had received the e-mail had clicked the link, and 75 had submitted their username and password. Had the e-mail gone unreported, and had the e-mail been a real attack, this could have cost Argonne hundreds of thousands of dollars in damages and lost productivity.



But how can you tell if a link is safe or not? **The common defense against this kind of attack is to move your cursor over the link without clicking.** Wait one or two seconds and what you'll see is a pop up window that will tell you exactly where that link will lead. If you look between the first two slashes following the http and the next slash, what you'll find is a code for the computer that the webpage is hosted on.



In this example, we had an e-mail that seemed to come from PayPal. But you can see that this isn't the PayPal address at all; an e-mail that seems to come from PayPal, and a link that goes somewhere else.

This is clearly a phishing attack. The best you can do is to delete the e-mail.

On most computers, only an administrator has the privileges to install software. Mac and UNIX systems typically have a separate login for installing software. But historically, Windows PC users have used a single login for both normal use and administrator tasks such as installing software. If you are using a PC and your user does not have administrator privileges, you are still vulnerable to loss of personal information, so you still need to be careful. But your computer is much less likely to be used as a platform to infect your coworkers' machines. The Laboratory has updated all PCs to separate user and administrator privileges.

Remote and Home Computing

Could your home computer be a back door? Absolutely!

Argonne incidents are often the result of infected home computers. Many employees use their home computers for work related to the Laboratory or to connect remotely to Argonne's systems using technology like VPN (Virtual Private Network). You can use the strategies listed below to protect your home computer as well as Argonne's computing systems.

To protect the Laboratory while computing remotely:

- Install virus protection and spam filters.
- Maintain your home computer monthly. Visit: <http://windowsupdate.microsoft.com>
- Install a home firewall. Use either:
 - A software firewall such as the Windows Firewall (in Microsoft XP) or ZoneAlarm. [Antivirus software](#) is available for free from the CIS Help Desk at 2-9999.
 - A hardware firewall such as a Linksys router behind your cable modem or DSL service.

Implement home wireless networks with caution! Verify your home wireless access point is in a secure configuration. Malicious users exploit open wireless access points to give an extra layer of anonymity by making it look like their attack came from your home!

Contact the CSPO or visit the [Cyber Security web page](#) to obtain a copy of the Cyber Security for Your Home Machine guide.

Data Restoration

Data loss can occur for multiple reasons, so a critical part of cyber security is the ability to restore a user's environment and data. Divisions have retention policies on how long backups are kept. Your environment and data should be part of a regular and reliable backup strategy that is to be used for disaster recovery only. Verify that backups are taking place and that your [CSPR](#) is aware of your computing environment and data needs.

This may involve:

- A local backup of your computer.
- A general file system strategy for your organization.

The backup strategy for your data must consider how quickly your environment must be restored and whether the data or system is sensitive or critical and so required to remain confidential or available.

Identifying and Reporting Potential Computer Incidents

You are Argonne's best mechanism for the identification and reporting of computer incidents. Although, monitoring capabilities built into Argonne's computing architecture can identify system attacks, the most accurate monitoring capability is yours. The best way to detect intruders is to prepare beforehand.

Recognize abnormal behavior

First, you should be able to recognize what is normal behavior of your computing system. That way you will be able to identify any abnormal behavior. You will be aware of "strange and unexplained" things that might happen. These include:

- Unexpected disk accesses
- Unexpected new files
- Unexpected increased disk space usage
- Unexplained open applications
- Unexplained printouts
- Unexplained sluggishness on your system

These things might be the result of normal operation or they may signal an intruder. Intruders and intruder software can operate, if attempted by a skillful attacker, with little consumption of resources. Learn how your computer system generally reacts and identify abnormal behavior

Incident Reporting

If you suspect an intrusion of your system has occurred:

- Don't panic.
- Contact your [CSPR](#) immediately. Every minute that passes provides more opportunity for the intruder to damage your computer, to use your computer to damage other computers, or allow time for others to find and exploit your vulnerability.
- Leave the computer ON.
- Do NOT modify any files.
- Do NOT close any applications.
- Start making notes of your discoveries and activities. Do not use a possibly compromised system to take notes or communicate about the suspected break in.
- Quarantine the system (leave it on with a sign on the monitor to warn against further use).

Reputable Sources

Only accept computer instructions from reputable sources like your system administrator or [CSPR](#).

Do not attempt to take care of the virus yourself. Far more damage to systems results from users trying to eradicate viruses and worms by themselves than from anything else.

Deterring Computer Theft

On average, 4 laptops are stolen from employees' hotel rooms and cars every year. Even here at Argonne, buildings with large common areas regularly experience the theft of components such as keyboards and mice.

For desktop computers:

- Use simple key locks with strong surface mount adapters to prevent equipment theft. Lock your office or lab when your computer is unattended for a significant amount of time.
- Turn on the computer software lock feature when you leave your computer for any reason.

For laptop computers:

- Notebook users must be particularly careful on travel. Airports and hotel lobbies are notorious venues for computer theft.
- Purchase Kensington or Kryptonite lock down cables.
- Do not save passwords that allow automatic login to systems/websites/intranet sites. This prevents unauthorized access to these areas in the event of computer theft.
- If you travel with your laptop in your car, store it in your trunk and not visible in the seat. Argonne employees' laptops have been stolen from their cars while parked in their driveway and hotel parking lots.
- When on travel for Laboratory business or pleasure, never let the laptop leave your sight including airport security checkpoints.

Top 10 Security Tips

1. Know your local [CSPR](#) and system administrators. Contact them before making configuration changes such as enabling file sharing, installing software, installing a modem, or setting up a wireless network access point. Comply with your divisional policy on making configurations.
2. Choose a complex password using the DOE guidelines, and keep it secret.

3. Use your computing and networking resources only for Laboratory-authorized activities.
4. Recognize and protect sensitive unclassified information.
5. Do not click on links in e-mails, docs, pdfs, and other electronic media unless you are absolutely sure of its source, destination, and/or function.
6. Don't use software from unknown sources or open questionable e-mail attachments.
7. Keep home computing secure to protect the Argonne computing infrastructure.
8. Make sure your computing environment is part of a reliable backup strategy.
9. Report unusual computer behavior immediately to your local [CSPR](#).
10. Keep your computer (particularly laptops) physically secure.

For more information visit the [Cyber Security Program Office](#) page or contact your local [CSPR](#).

Computer User Agreement

This course covered several principles that govern the use of Argonne Information Technology (IT) assets.

The Argonne National Laboratory Computer User Agreement is a concise list of these principles and policies. By taking this course and exam, you will be expected to comply with and abide by the conditions of the agreement as well as follow all policies set forth in the [Cyber Security Program Plan \(CSPP\)](#).

Please open and review the [Computer User Agreement](#).

Data Awareness Survey

Please fill out the survey and fax it back to the **Argonne Cyber Security Office at (630) 252-9689**. Definitions for each term are provided on subsequent pages.

Name: _____

Signature _____

Badge: _____ Division: _____ Date: _____

In your responsibilities at the Laboratory, do you work with the following types of sensitive data in electronic form?

- Personally Identifiable Information (PII)
- Export Controlled Information (ECI)
- CRADA/WFO
- Unclassified Controlled Nuclear Information (UCNI)

If you do work with the data types described above, please identify where the data is stored.

- Laboratory Desktop Computer System
- Laboratory Laptop Computer System
- Divisional File Share
- Laboratory Business Systems
- Removable Media
- Personally Owned Computer System

If you DO NOT work with any of the above, please check the following checkbox.

- I do not work with any of the above.

Definitions:

Personally Identifiable Information (PII)

An individual's first name or first initial and last name with any of the following: Social Security Number, Passport, Credit Card, Clearance Levels, Bank Numbers, Biometrics, Date of Birth, Place of Birth, Mother's Maiden Name, Criminal Record, Medical Records, Financial Records, Educational Transcripts

Export Controlled Information (ECI)

Any communication of technical data, subject to export controls, to a foreign national, whether it takes place in the United States or abroad. Providing any technical information or data to a foreign national, whether done verbally, by mail, by telephone or facsimile, through visits or workshops, or through computer networking, is an export. If a foreign national observes equipment or a process, which also may constitute an export of technical data, if significant details are revealed.

CRADA / WFO

CRADAs are cooperative research and development agreements between Argonne and industrial partners that contribute to the goals of each party. A CRADA may be cost shared between the industrial partners and Argonne or may be 100% funded by the industrial partners. While it is generally the case that companies are able to retain rights to their own inventions made under a CRADA, there are exceptions. Similarly, the rights to intellectual property created by the Laboratory under a CRADA are retained by Argonne. However, the industrial partner does have a right to an option to license Argonne's inventions. It is best to defer to OTT or the Legal Department in all discussions of intellectual property rights.

Work-for-Other agreements (WFOs) are a mechanism through which industry can utilize the unique expertise and facilities at Argonne National Laboratory. In this type of arrangement the industrial sponsor pays 100% of the cost of the work to be performed by Argonne. Under certain conditions, a company may take title to inventions created by Argonne under the SRO. Some key points in such arrangements include product, general and IP indemnification, advance payment requirements and the fact that Argonne may not compete with the private sector for such work. Work to be performed by Argonne via a successfully funded SBIR/STTR proposal is also a SRO; however, in this case, it is federally funded and different terms will apply.

Unclassified Controlled Nuclear Information (UCNI)

Unclassified Controlled Nuclear Information is certain unclassified Government information whose unauthorized dissemination is prohibited under section 148 of the Atomic Energy Act. Such information may concern details about the design of nuclear production or utilization facilities; security measures for protecting such facilities, nuclear materials contained in such facilities, or nuclear material in transit; or the design, manufacture, or utilization of nuclear weapons or components that were once classified as Restricted Data.

Laboratory Desktop Computer System

A Laboratory desktop computer system is the computer that you use to conduct your Laboratory business on. These systems are managed by your divisional IT Administrator and often do not leave your office.

Laboratory Laptop Computer System

A Laboratory laptop computer system is the mobile computer that you use to conduct your Laboratory business on. These systems are managed by your divisional IT Administrator and may be used offsite while on travel from the Lab.

Divisional File Share

A divisional file share is a central location for you to store and save your files that has been established by your divisional IT Administrator.

Laboratory Business Systems

A Laboratory business system is a central application that is used to conduct Laboratory business functions. Examples include: HR Application, PARIS, FAVOR, Financial System, etc.

Removable Media

Removable media refers to storage media which can be removed from its reader device, conferring portability on the data it carries. Examples include: Thumb drives, CDs, DVD, etc.

Personally Owned Computer System

A personally owned computer system is a computer that is owned and operated by the employee and may be used to conduct Laboratory business while at home or on travel.