



OFFICE OF THE CHIEF INFORMATION OFFICER

Computer Security Training for New DOL Users



Course Introduction

Welcome to the Information Systems Security Awareness course. The Federal Information Security Modernization Act, or FISMA, and the Office of Management and Budget, or OMB, Circular A-130 require that all users of Federal computer systems be trained in information systems security concerns.

This course fulfills that requirement. Federal law requires that all users annually take information security awareness training. This course is designed to help you understand the importance of information systems security (ISS), its guiding principles, and what it means for your agency.

Purpose and Objectives

Purpose:

This course will identify potential risks and vulnerabilities associated with federal information systems, review your role in protecting these systems, and provide guidelines to follow at work and at home to protect against attacks on information systems.

Objectives:

- Enable employees to identify potential risks and vulnerabilities associated with Federal information systems
- Enable employees to review their roles in protecting these systems
- Provide guidelines to follow at work and at home to protect against attacks on information systems

Overview of Information Systems Security

The goal of Information System Security (ISS) is to protect our information and information systems. Information systems security is defined as,

With three major IT cornerstones that are measures that protect and defend information and information systems by ensuring their:



Availability - means that information services are accessible when they are needed.

Integrity - protection from unauthorized modification or destruction of information.

Confidentiality - safeguards information from being accessed by individuals without the proper clearance, access level, and need to know.

Other important terms to be familiar with are:

Authentication - means a security measure that establishes the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

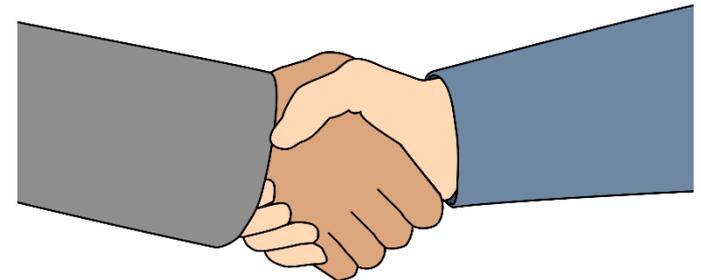
Non-repudiation - means assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. As an authorized user, you are responsible for contributing to the security of all Federal computer systems.

You must abide by these principles of information system security in your daily work routine to protect Federal information and information systems.

Employee Acceptance at Login to a DOL System

I agreed to What?

- All information belongs to DOL:
 - Information may be monitored, intercepted, recorded, read, copied or captured by authorized personnel and given to law enforcement officials if potential evidence of crime
- Use = Consent means
 - There is no expectation of privacy
- Users are responsible for safeguarding and protecting data, including PII, equipment and resources



Appropriate Use of IT Resources

Examples of Appropriate Use	Examples of Inappropriate Use
Use does not result in loss of employee productivity.	Use that could cause congestion, delay, or disruption of service to government systems or equipment.
Use must not interfere with official duties.	Creation, copying, or transmission of unauthorized mass mailing, chain letters, pyramid schemes, daily jokes and inspirational messages.
Taking extra steps to protect Personally Identifiable Information (PII) at all times.	Creation, download, viewing, storage, copying of sexually explicit or sexually-oriented materials.
Encrypting PII prior to transmitting outside the DOL network.	Conduct illegal activities, i.e., gambling, illegal weapons, terrorist activities.

Threats and Vulnerabilities

Federal information and information systems must be protected from threats to minimize vulnerabilities.

- A **threat** is any circumstance or event that can potentially harm an information system by destroying it, disclosing the information stored on the system, adversely modifying data, or making the system unavailable.
- A **vulnerability** is a weakness in an information system or its components that could be exploited.

Vulnerabilities exist when there is a flaw or weakness in hardware or software that could be exploited by hackers. An example of a vulnerability is a flaw in the coding of software. To correct such vulnerabilities, vendors issue fixes in the form of patches to the software.

To address these vulnerabilities on your home computer system, update your operating system and other software as patches become available.

Environmental Threats

One type of environmental threat is a natural event; some natural events can pose a threat to your system and information. These threats include:

- Lightning
- Fires
- Hurricanes
- Tornadoes
- Floods

Another kind of environmental threat is a system event. A system's environment, including poor building wiring, insufficient cooling, or power outages can also cause harm to information systems.

Human Threats: Internal vs. External

The greatest threats to Federal information systems are internal, from people who have working knowledge of, and access to, their organization's computer resources. An insider is any person who has legitimate physical or administrative access to the computer system. Insiders can misuse or exploit weaknesses in the system. Others, due to lack of attention, or lack of training and awareness, can also cause serious damage.

Internal threats can be:

- Careless, malicious, or disgruntled users
- Self-inflicted, unintentional damage, such as accidents or bad habits

External threats can be:

- Individual hackers
- Representatives of foreign countries
- Organized crime

Data Classification

Information is a critical asset to the U.S. Government. Proper protection of Federal information is essential to information systems security. Outside of the national security environment, there are two general classes of information: sensitive and non-sensitive.

Sensitive Information:

Inadequate protection of sensitive information, may cause the loss of confidentiality, integrity, or availability and could be expected to have a serious, severe, or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Examples: Sensitive agency data and protected Personally Identifiable Information such as Social Security Numbers (SSNs), dates of birth, medical records, credit card numbers.

Non-sensitive information:

- Information cleared for public release
- Internet web site pages, available to the general public



Personally Identifiable Information

Personally Identifiable Information (PII) is defined as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Non-Sensitive PII is defined as PII whose disclosure cannot reasonably be expected to result in personal harm. Examples include first/last name; business e-mail address; business address; business telephone; and general education credentials that are not linked to or associated with any protected PII.

Protected PII is defined as PII whose disclosure could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited to, social security number; credit card number; bank account number; residential address; residential or personal telephone; biometric identifier (image, fingerprint, iris, etc.); date of birth; place of birth; mother's maiden name; criminal records; medical records; and financial records. The conjunction of one data element with one or more additional elements increases the level of sensitivity and/or propensity to cause harm in the event of compromise.



Social Engineering

Avoid falling victim to these scams. Protect yourself, your fellow employees, and Federal systems, by following these security tips:

- If the request for information is through a survey, tell the person that you do not participate in surveys
- Do not give out personal information about yourself or other Federal employees, including names, positions, telephone numbers, and passwords
- Do not give out computer systems or network information
- Do not follow any instructions from unverified personnel



When contacted, document the interaction

- Attempt to verify the identity of any individuals who approach you
- Try to obtain as much information about the person as possible.
- If Caller ID is available, write down the caller's telephone number
- Take detailed notes of the conversation

Contact your agency Information Systems Security Officer (ISSO) or service desk with any questions or for additional guidance.

Phishing

Phishing is one type of social engineering that uses e-mail or websites to trick you into disclosing personal or sensitive information with the intention to steal your identity (identity theft), run up bills or commit crimes in your name, or access your organization's computer systems. Examples include:

- Credit card numbers
- Bank account information
- Your Social Security Number
- Passwords



Phishers try to deceive you by sending e-mails or pop-up messages that appear to be from:

- Your Government agency
- Your Internet Service Provider (ISP)
- Your bank
- Some other legitimate business or organization

Phishing Continued

Phishing attacks often consist of e-mails containing a link that redirects a person to a spoofed website (e.g. Banks, IRS, PayPal, etc.). Cybercriminals trick users into providing their credentials, allowing the criminals undetectable access to the user's accounts. Phishing attacks attempt to get ANY sensitive information from users.

Note: Phishing attacks are increasingly common, because they are effective. Read your emails carefully so that you don't accidentally click on a dubious email.

The image shows a screenshot of an email interface with several annotations in green boxes and arrows pointing to suspicious elements:

- Urgency:** A green box with an arrow pointing to the subject line: "Change of password required Immediately".
- Hover over the link to reveal the link is not legitimate:** A green box with an arrow pointing to the underlined text "Change Password".
- Questionable Signature:** A green box with an arrow pointing to the signature block, which includes the text "Sincerely," and a small icon of a red 'x' in a box next to the name "IT".
- Link:** A grey box highlights a long, complex URL: `http://password-changes.phishwall.net/cmjvaxbpzw50x2lkpti3mtixmdk0mczjyw1wywlnb19ydw5fawq9mjpg0ndm3jmfjdgvlj1jbgjzayz1cmw9ahr0cdovl2f1zgl0lmtub3diztquy29tl2tinc5odg1s`. Below the URL is the text "Click to follow link".

The email header includes the following information:

- From: IT@doc.gov
- To: Meyer, Gail
- Cc:
- Subject: Change of password required Immediately
- Sent: Mon 12/1/2014 8:45 AM

The main body of the email contains the following text:

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.

Please click here to do that:

Change Password

Please do this right away. Thanks!

Sincerely,
IT

Phishing Continued

Avoid becoming a target for phishers. Follow these security tips:

- Do not access the web by selecting links in e-mails or pop-up messages, if they ask for personal or financial information.
- If an e-mail appears suspicious, do not click on links or open attachments.
 - Send the email as an attachment to both SPAM@dol.gov and DOLCSIRC@dol.gov and then simply delete the e-mail.
 - To send as an attachment: Open a new email in Outlook -> Select “Attach Item” from the toolbar -> Choose the “Outlook Item” option -> Find the suspicious email in the list, then click “OK” to attach
- Never provide your password, PIN or other personal information through email or pop-up.
- Remember, legitimate companies do not ask for personal information via e-mail. If you are concerned about your account, contact the organization in the e-mail using a telephone number you know to be genuine. If you want to check your account status online, type the web address directly into your browser, or use your personal bookmark.
- If you believe you have a security issues or think you may have clicked on a potentially malicious link, immediately contact your Agency’s Information Security Officer (ISO). You can find a list here on [LaborNet](#). If your ISO is not available, please reach out directly to the OCIO security incident response team at DOLCSIRC@dol.gov.

Spear Phishing

Spear phishing is a type of targeted phishing. Spear phishers send e-mails that appear to be from inside your organization. For example, a message might appear as if it came from your

- Supervisor
- Human Resources
- The IT department
- The message might include requests for user names or passwords

Spear phishers attempt to gain access to an organization's entire network, putting the security of that organization's information at risk. Or, spear phishers may make you a victim of identity theft.

Protect yourself and Federal information systems from spear phishers by following these security tips:

- Never give out your password to anyone!
- IT, or any legitimate person from your organization, will never ask you for your password. If someone from the IT department requires access to your computer, they will use their administrator user name and password
- Never reveal any information system related information, or personal information, in response to an unsolicited e-mail. This includes user name, address, or date of birth.

Creating a Secure Password

Follow these general password guidelines to protect Federal information systems from being compromised. Using these guidelines at home keeps your home computer secure as well.

Passwords are only for your individual use to your personal accounts at work and at home.

No one from the DOL will ask you for your Password.

Do not Share your Password for any reason.

Apply the password policies as noted in the Computer Security Handbook (CSH) Volume 7:

- Passwords must be at least 8 characters long,
- Are to be changed on first logon for a DOL account
- Have at least one upper case,
- Have at least one lower case, and
- Have at least one number,

Take extra care to ensure Passwords Do Not:

- Have Dictionary words or common names (including but not limited to, Betty, Fred, Rover)
- Use portions of associated account names (including but not limited to, user ID, login name)
- Use consecutive character strings (including but not limited to, abcdef, 12345)
- Use simple keyboard patterns (including but not limited to, qwerty, asdfgh)
- Use generic passwords {including but not limited to, password consisting of a variation of the word "password" (including but not limited to, P@ssw0rd1)}



U.S. DEPARTMENT OF LABOR
Office of the Chief Information Officer



**IDENTIFICATION AND AUTHORIZATION
POLICY, PROCEDURE AND STANDARDS**

VERSION 1.0

DECEMBER 2017

Physical Security

Physical security, sometimes referred to as guns, gates, and guards, protects an entire facility.

You are responsible for knowing your facility's physical security policies, and for following them. The agency has procedures for:

- **Gaining entry to a secure area**
- **Securing your work area at night**
- **During emergencies**

Protect your facility by following these general security tips

- **Always use your own badge or key code to enter a secure area**
- **Never grant access for someone else using your badge or key code**
- **Challenge people who do not display badges or passes**
- **Report any suspicious activity that you see to your agency ISSO**

Identity Theft

Identity theft occurs when someone uses your identifying information, without your knowledge, to commit fraud or other crimes. Such information may include your:

- Name
- Address
- Social security number
- Bank or credit card account number

Identity thieves can use the information they obtain to:

- Open credit card accounts
- Take out loans
- Drain a bank account without your knowledge

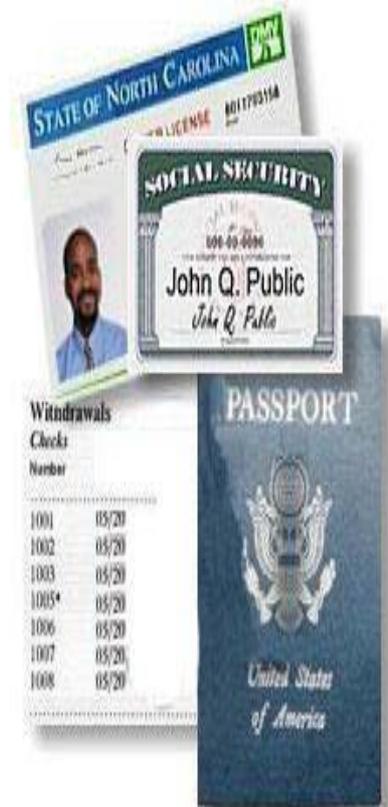
Identity Theft Continued

Follow these guidelines:

- Avoid using common names or dates when creating passwords or personal identification numbers (PINs).
- Pick up your mail promptly.
- Shred all personal documents and mail that contain sensitive information, especially pre-approved credit card offers.
- Do not carry your Social Security card or passport in your purse or wallet unless absolutely necessary.
- Order copies of your credit report every year.

Do the following if you discover you are a victim of identity theft?

- Contact all three credit reporting companies (Equifax, Experian, and Trans Union) and have your account marked for fraud.
- Contact your banks, credit card issuers, and other creditors to notify them of the identify theft.
- Monitor your credit card statements for unauthorized purchases.
- Report the crime to the local police. If you do not make this report, you may not be able to recover your money, even if the perpetrators are identified.



Withdrawals	
Checks	
Number	
1001	05/20
1002	05/20
1003	05/20
1005*	05/20
1006	05/20
1007	05/20
1008	05/20

Malicious Code

Malicious code describes software that is purposely designed to do damage to, or cause unwanted behaviors in, a computer system.

Common types of malicious code are:

- Viruses
- Trojan horses
- Worms

Malicious code can also appear as a macro or script, it could come as:

- E-mail attachments
- Downloaded files from the Internet
- Result of visiting an infected website that automatically downloads malicious code

Malicious code can:

- Corrupt files
- Erase your hard drive
- Enable a hacker to gain access to your computer system

Malicious Code Continued

Protect your computer system from viruses, both at work and at home, by following these simple security tips:

- Don't assume an attachment is safe just because a friend or coworker sent it.
- Before launching an e-mail attachment, scan it with up-to-date, anti-virus software. Your system should be set up for your anti-virus software to scan your system daily.
- If you receive a suspicious message, delete it, without opening it.
- Turn off the option for automatic downloading of attachments. This will enable you to scan each attachment before it can infect your system.



Ransomware

Type of malware that prevents or limits user from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payments methods such as bitcoins to get a decrypt key.

Protect your computer system from ransomware, both at work and at home, by following these simple security tips:

- Do not provide personal information when answering an email, unsolicited phone call, text message or instant message. Phishers will try to trick you into installing malware, or gain intelligence for attacks by claiming to be from IT.
- Routinely backup data
- Ensure your antivirus software is up-to-date
- Keep up with patches



Computer Viruses

If your system is acting erratically or running abnormally slow, it may contain a virus or other malicious code. Note that the system may contain a virus, even if it appears to be virus free.

Follow these security tips to protect your computer from viruses and malicious code:

- Scan all external files before uploading to your Government computer, or the computer network, if your organization permits this practice.
- Follow DOL policies with respect to loading outside files onto your workplace computer. This includes files brought in on external media, such as thumb drives, CDs, or floppy disks, as well as files e-mailed from your home computer to your work e-mail address.

If you discover or suspect that a virus has infected your system, do not e-mail the infected file to anyone. Immediately contact your agency ISSO or service desk for assistance.

Internet Hoaxes

Internet hoaxes are e-mail messages, often designed to influence you to forward them to everyone you know by

- Warning of new viruses
- Promoting moneymaking schemes
- Citing fictitious causes



By encouraging mass distribution, hoaxes clog networks and slow down Internet and e-mail services for computer users. A forwarding request can also be a part of a distributed denial-of-service (DDoS) attack, intended to bring down computer networks by flooding them with traffic.

By forwarding an e-mail to large groups of other users, you are helping hackers execute their attack.

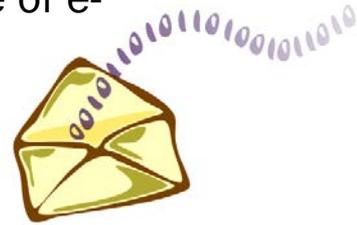
You can limit the effect of e-mail hoaxes by following these security tips:

- If an e-mail requests that you forward the message to everyone in your address book, it is probably a hoax; do not forward it.

Ethical Guidelines for Use of E-mail

Although DOL may permit some incidental e-mail use from your Government computer, e-mail is for official business. Follow these guidelines for ethical use of e-mail:

1. E-mail use must not adversely affect the performance of official duties.
2. E-mail use must not reflect poorly on the federal government.
3. Do not use government e-mail to sell anything.
4. Do not send chain letters, or offensive e-mails, including: pornographic, political, racist, or sexist e-mails.
5. Do not send or forward mass e-mails; these overburden the system.
6. Do not send or forward (these also overburden the system): jokes, pictures, or inspirational stories.
7. Avoid using "Reply All" unless it is absolutely necessary, especially with e-mails with large address lists; for any e-mail you send, select the addressee list carefully.
8. Personal e-mail use may be authorized if it is of reasonable duration and frequency, preferably on an employee's personal time, such as on a lunch break.
9. E-mail is also permissible when it serves a legitimate public interest, such as allowing an employee to search for a job in response to federal government downsizing.
10. Locally, personal e-mail use guidelines may be more restrictive.
11. Confirm your organization's guidelines prior to using your work email for personal matters.



Removable Media

Removable media includes

- CDs
- DVDs
- Thumb drives
- Flash drives
- External hard drives



Removable media that contains sensitive information must be properly

- Labeled
- Stored
- Encrypted
- Purged/Degaussed (when discarded)

If the media contains PII or other sensitive data, including government information not cleared for public release, the information must be encrypted. Contact your agency ISSO for additional information on proper labeling of removable media.

Be careful how you discard of CDs or other removable media. Media that contains sensitive information must be purged/degaussed before it is discarded. Merely deleting sensitive data does not prevent it from being recovered. The most common purging method is using an approved software tool that repeatedly overwrites the entire media to completely destroy any recoverable remnants of the original information.

Mobile Computing Devices

Be extra vigilant when storing data on PDAs and other mobile computing devices, such as laptops. Because of their small size and portability, these devices are especially vulnerable to security risks.

All PDAs and other mobile computing devices connecting to government systems must be in compliance with federal policy. Please note that the government considers laptop computers as mobile computing devices.

All laptops that store PII must be secured using a whole-disk encryption solution to protect the sensitive information stored on them.

All sensitive data must be encrypted in accordance with the data's sensitivity level. This includes all PII, such as:

- Social Security Number
- Dates and places of birth
- Mothers' maiden names
- Biometric records

If a device is lost or stolen, immediately report the loss to your agency ISSO and the Enterprise Service Desk.



Fax Machines

Before transmitting sensitive information over a fax machine

- Ensure that the recipient is at the receiving end, ready to pick up the fax immediately
- Use the correct cover sheet for the sensitivity of the information you are faxing
- After sending the fax, contact the recipient to confirm receipt

Never transmit sensitive information via an unsecured fax machine.



Telework and Wireless Technology

- You must receive approval for telework and must satisfy all of the requirements in your agency's policies and guidelines. There are strict guidelines for telecommuting; follow your organizations policy for telework or when working remotely.
- You must implement appropriate security measures, as outlined in your telework agreement.
- You must sign a telework agreement.
- You must sign a safety checklist.
- You must always take care to protect any data involved in your telework.
- Only take sensitive information off-site with management approval, and only in limited quantities.



E-Commerce and Cookies

A cookie is a text file that a web server puts on your hard drive. Though sometimes useful, enabling cookies can pose a security threat, the most serious being when a cookie "saves" unencrypted personal information, such as your credit card numbers or Social Security Number.

Cookies can also track your activities on the web; this also poses a security risk, and may lead to a potential invasion of your privacy.

Both in the office and at home, shop online wisely and follow these security tips:

- Use cookies with caution
- If your organization doesn't configure your cookies setting, set your browser preferences to prompt you each time a website wants to store a cookie
- Only accept cookies from reputable, trusted websites
- Confirm that any e-commerce site conducts its business over an encrypted link before providing any personal information
- An encrypted link is indicated by "h-t-t-p-s" in the URL name
- Make sure that an icon is visible that indicates the encryption is actually functioning
- Note that not all https sites are legitimate; you are still taking a risk by entering your information online

Safe at Work, Home or on the Road

You can be held responsible for

- Actions taken in your name
- Information accessed via your account
- Always log off at night
- If taking a break
 - Log off
 - Lock the workstation

Laptop is attractive, valuable equipment

- Keep it with you at all times
- Use anti-theft cables

Portable data is attractive, too

- Encrypt sensitive files
- Lock files

Home Security

There's more to know about safeguarding your home computer. Follow these security tips to keep your home computer secure:

- Download and install the latest system and application security updates and patches,
- Install a good anti-virus program and keep it up-to-date,
- Regularly scan files for viruses,
- Install spyware protection software,
- Turn on firewall protection,
- Back up your files on a regular basis.



Sign Section VI User Agreement

When finalizing the Initial Network Access Request (INAR) form to gain access to a DOL account you will acknowledge by signing Section VI User Agreement that you understand that you are personally responsible for your use and any misuse associated with your DOL network account as shown in the image below:

SECTION VI USER AGREEMENT	
<p>As a user of the U.S. Department of Labor's (DOL) information systems, I understand that I am personally responsible for my use and any misuse associated with my user account and passwords. I have read the Computer Security Training for New DOL Users and understand and acknowledge that I must comply with the requirements set forth therein. I further understand and agree that by accessing a U.S. Government information system and signing this form, I must comply with the requirements set forth in the DOL User Rules of Behavior, Version 4.8 and other pertinent policies for information systems.</p>	
User Signature _____	Date <input type="text"/>
Print Name <input type="text"/>	Phone Number <input type="text"/>