Rules of Behavior – Acceptable Behavior and Penalties

Rules of Behavior establish expected and acceptable computing behaviors. Because written guidance cannot cover every contingency, users are also required to use sound judgment and the highest ethical standards in their decision-making.

USDA will take corrective action and/or enforce the use of penalties against any user who violates any USDA or Federal system security policy, using any and/or all of the following:

- Corrective actions (taken in accordance with existing rules, regulations, and laws) include written reprimands, temporary suspension from duty, reassignment or demotion, and termination of federal employment.
- Suspension of system privileges.
- Possible criminal prosecution.

What you should know.

The following unofficial activities are prohibited on any information system owned or operated on behalf of USDA or any government-issued phones, tablets, and other devices:

- Gambling.
- Intentionally visiting and downloading material from pornographic websites.
- Lobbying Congress or any government agency.
- Campaigning – political activity.
- Any type of continuous audio or video streaming from commercial, private, news, or financial organizations, except as expressly authorized by management.
- Activities that relate to any type of outside employment.
- Endorsement of any non-government products, services, or organizations.
- Apps such as: Confide, Signal, Telegram, and WhatsApp.

Your Role in Social Engineering

Social engineering is a hacking technique that relies on human nature.

Understanding social engineering behaviors will enable you to recognize them and avoid providing important security information to unauthorized sources.

Preventing social engineering:

- Verify identity.
- Do not give out passwords.
- Do not give out employee information.
- Do not follow commands from unverified sources.
- Do not distribute dial-in phone numbers to any computer system except to valid users.
- Do not participate in telephone surveys.

Reacting to social engineering:

- Use Caller ID to document phone number.
- Take detailed notes.
- Get person's name/position.
- Report incidents.

Rules of Behavior – Access

- Users are responsible and accountable for any actions taken under their user ID.

- Users are prohibited from using peer-to-peer (P2P) file sharing unless specifically approved by management in writing.

The Office of Management and Budget (OMB) requires all Agencies to develop guidance on the use of peer-to-peer applications.

Contact your security point of contact for further information on your specific policy regarding the use of peer-to-peer applications.

What you should know.

Users shall:

- Follow established procedures for accessing information, including the use of user identification, user authentication, passwords, and other physical and logical safeguards.
- Follow established channels for requesting and disseminating information.
- Access only those files, directories, and applications for which access authorization by the system administrator has been granted.
- Use government equipment only for approved purposes.

In addition, users shall **NOT:**

- Give information to other employees or outside individuals who do not have access authority.
- Store sensitive or confidential information on a system unless access control safeguards (e.g., passwords, locked rooms, and protected local area network (LAN) storage areas) are used.
- Use their trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties.
- Browse other users' files (i.e., what can be accessed).

Rules of Behavior - General Software

Users shall not install unauthorized, standard, public domain, or shareware software on their computer without approval from the appropriate management official. Computer users must protect USDA-owned software and equipment from malicious software.

Users shall:

- Comply with all software licensing agreements and Federal copyright laws.

In addition, users shall NOT:

- Use USDA-purchased software on personally-owned or non-USDA computers unless authorized.
- Alter the configuration on Government computer equipment, including installing or uninstalling software or peripherals, unless authorized.
- Download, install or run security programs or utilities that might reveal weaknesses in the security measures or access privileges of any system unless otherwise expressly authorized.

Basic User Ethical Guidelines

There are eight basic generally accepted ethical guidelines that should govern your actions when using a government computer system.

Ethical guidelines

- Do not use computer for harm.
- Do not interfere with other's work.
- Do not snoop in other's files.
- Do not use a computer to commit crimes.
- Do not use or copy unlicensed software.
- Do not steal intellectual property.
- Do not use a computer to pose as someone else.
- Do not use computer resources without approval.

Rules of Behavior – Accountability

In addition to adhering to ethical guidelines, all users are accountable for actions related to information resources entrusted to them.

Users shall:

- Behave in an ethically, informed, and trustworthy manner when using systems.
- Be alert to threats and vulnerabilities such as malicious programs and viruses.
- Participate in IT security training and awareness programs.
- Not install or use unauthorized software on USDA equipment.
- Comply with all software licensing agreements and not violate Federal copyright laws.
- Know that your system may be monitored and that there is no expectation of privacy on USDA IT resources.

What you should know.

In addition, users shall prevent others from using their accounts by:

- Logging out or locking the screen when leaving the vicinity of their terminals or PCs.
- Setting a password on automatic screen savers.
- Helping to remedy security breaches, regardless of who is at fault.
- Immediately notifying the system administrator whenever there is a change in role, assignment, or employment status and/or when access to the system is no longer required.
- Complying with a system's rules of behavior when accessing external systems.
- Reading and understanding banner pages and end user licensing agreements.

Rules of Behavior – Integrity

Users must protect the integrity and quality of information. This includes, but is not limited to:

- Reviewing quality of information as it is collected, generated and used to ensure that it is accurate, complete, and up-to-date.
- Taking appropriate training before using a system to learn how to correctly enter and change data.
- Protecting information against viruses and similar malicious code by:
  - Applying security updates as required, and using up-to-date anti-virus software, if not controlled at the agency/enterprise level
  - Avoiding use of unapproved software, such as shareware and public domain software.
  - Discontinuing use of a system at the first sign of virus infection.
- Never knowingly enter unauthorized, inaccurate, or false information into a system.

Rules of Behavior – Email: Appropriate Email Use

The following rules apply regarding email activity:

- Automatic filters will be in place to help prevent inappropriate and offensive messages from passing through USDA email gateways.
- Any email on a government email system is the property of the government and may become an official record.
- The use of IT resources constitutes consent to possible monitoring and security testing. Monitoring and security testing ensures proper security procedures and appropriate usage are being observed for USDA IT resources.
- Monitoring of email and other IT resources by management will be done only in accordance with established USDA policies and guidelines.
- Users are prohibited from using USDA IT resources to send, receive, retain, or proliferate any message or material that is fraudulent, inappropriate, offensive, harassing, or is of a sexual nature.

What you should know.

Email is for official business. Your organization may also permit some incidental and casual email use. Guidelines on the types of personal email use that may or may not be authorized are as follows:

- Email use may not adversely affect the performance of official duties.
- Email use must not reflect poorly on the government.
- You may not use government email to send pornographic, racist, sexist, or otherwise offensive emails, send chain letters, or sell anything.
- Email use must not overburden the system, as happens when you send mass emails.
- To keep networks open and running efficiently, don't forward jokes, pictures, or inspirational stories.
- Similarly, avoid using "Reply All" unless it is absolutely necessary.
- Personal email use may be authorized if it is of reasonable duration and frequency, preferably on employees' personal time, such as on a lunch break.
- Email is also permissible when it serves a legitimate public interest, such as allowing employees to search for a job in response to federal government downsizing.

Tips for Creating a Secure Password

John thinks having to change passwords frequently and memorizing them is complicated and inconvenient. So, he writes them down and leaves them under his computer keyboard. Maybe John just needs some tips for creating secure passwords that he can remember?

Many federal information systems still identify and authenticate users by his or her user ID and password. The user ID and password determines the user's right to access the system.

Remember, it is your responsibility to ensure that all activity performed under your user ID is appropriate use of federal information systems resources.

What you should know.

It is important to create a complex password in order to protect government information systems from being compromised.

- Combine letters, numbers, special characters. (Ex: !,@,#,$).
- Use alphanumeric combinations or phrase associations. (Ex: P@$$w0rd T1p$).
- Avoid words or phrases that can be found in the dictionary.
- Avoid using personal information. (Ex: birthday, home address, phone number).
- Memorize password and refrain from writing it down.
- Change passwords regularly.

Backups, Storage, and Labeling

A large amount of federal information is stored on removable media such as CDs, USB drives, or removable hard drives and you need to take extra precaution to protect them from loss or theft.

Important files MUST be backed up regularly and stored in a secure location to minimize the loss of data if your hard drive crashes or is infected by a virus. Store all removable media in solid storage containers, such as metal cabinets, to protect against fire and water damage.

It is very important to label all removable media, including backups, and the contents of the media, to reflect the classification or sensitivity level of the information the media contains. Removable media must be properly marked and stored according to the security classification of information it contains. When you no longer need the information, you should not erase, or "sanitize" it. Removable media must be degaussed or destroyed if they are not reused at the same or higher classification level of the system in which they were used.

Follow your agency's policies regarding handling, storage, labeling, and destruction of removable media.

Rules of Behavior – Backups, Storage, and Labeling

Computer systems and media must be protected from environmental hazards such as fire, water, heat, and food spills. They must also be protected from theft, unauthorized alteration, and careless handling.

What you should know.

Users shall:

- Use physical and logical protective measures such as the following to prevent loss of availability of information and systems.
- Ensure that there are backups of information for which they are responsible.
- Protect systems and media where information is stored.
- Store media in protective jackets.
- Keep media away from devices that produce magnetic fields (such as phones, radios, and magnets).
- Follow contingency plans.

Incident Reporting

Each user is responsible for reporting any form of a security violation, whether waste, fraud, or abuse through the USDA incident reporting mechanism.

What you should know.

Users shall:

- Report security incidents, or any incidents of suspected fraud, waste, or misuse of USDA resources or release of USDA personally identifiable information (PII) to the USDA Help Desk (1-888-926-2373) or PII Hotline (1-877-PII-2-YOU), or to the appropriate agency IT Information Security Program Manager.
- Report security vulnerabilities and violations as quickly as possible to the USDA Help Desk (1-888-926-2373) or USDA PII Hotline (1-877-PII-2-YOU), or to the appropriate agency IT Information Security Program Manager so that corrective action can be taken.
- Take reasonable action immediately upon discovering a violation to prevent additional damage, such as logging out of a terminal or locking up property.
- Cooperate willingly with official action plans for dealing with security violations.

International Travel with Government Furnished IT Equipment

Remote client devices such as laptop computers, cell phones and tablets used to perform work from foreign locations introduce additional risks to USDA information and information systems; therefore, these devices have additional security requirements than those operating within USDA controlled areas and those operating from remote locations within the United States and its territories.

Foreign governments are very skilled at collecting information even from devices that are turned off. Devices and sensitive information taken to foreign countries are susceptible to infection, compromise, and theft. Infected devices may not be discovered upon return and, if reconnected to USDA networks, may compromise the security of additional information.

What you should know:

- Only employees and contractors with official government business requiring international travel and those whose permanent duty station is outside the U.S. can take government furnished IT equipment out of the country.
- If you are going on personal international travel, leave your government furnished IT equipment secured at your current work location.
- If you have official government business requiring international travel, please refer to the latest USDA and Forest Service requirements for taking government furnished IT equipment out of the United States and its territories.

Privileged User Guidelines - Do's

As a Privileged User I shall:

- Abide by the provisions of the USDA IT/IS Rules of Behavior for General Users except those variations required to perform authorized privileged user activities.
- Limit the performance of privileged user activities to privileged user account(s).
- Consent to monitoring and search of any IT/IS equipment used while in or brought into or removed from USDA-owned, controlled, or leased facilities.
- Complete Information Security Training.
- Successfully complete any specialized training required by USDA that is related to competent and secure operation of IT and IS for which I have privileged user status.
- Submit to additional investigation and monitoring of my privileged user activities as required to ensure integrity of my privileged user activities.
- Immediately report any anomalous incident, including errors and oversights related to my privileged user activities, to my Information System Security Officer (ISSO), Information System Security Program Manager (ISSPM), or Assistant Chief Information Officer (ACIO) according to the appropriate USDA Cyber Security Incident Management Procedures.
- Use my privileged user role and access to perform only authorized privileged user activities for the benefit of the USDA.
- Protect my "root" or "super user" account including passwords and privileges at the highest level of data that it secures.
- Change my privileged user account password every ninety (90) days or as required for security reasons.
- Protect all output whether hardcopy, electronic, or optical according to USDA policy.
- Perform virus and integrity scanning of any media that is to be used to transfer information into an USDA system.
- Notify the ISSO when my privileged user access to the system is no longer needed (e.g. transfer, termination, leave of absence, or for any period of extended non-use). If I am an ISSO, then I will notify my ACIO when my privileged user access is no longer needed.

Privileged User Guidelines - Don'ts

Unless required as part of my official duties as a Privileged User of USDA IT/IS, I will NOT:

- Share my privileged user access or privileges with any unauthorized person.
- Use my privileged user access or privileges to "hack" any IT/IS (networked or non-networked).
- Attempt to gain access to data for which I am not specifically authorized, to include e-mail and users' files in their home directories.
- Use my privileged user access for non-Government business.
- Introduce any software or hardware that has not been approved through Change Management Process into USDA IT/IS, systems or networks.
- Use any USDA communications, transmission, processing, or storage components for unauthorized purposes.
- Disclose, without authorization, any personally identifying information (PII) that I access or learn as a result of my privileged user duties and activities.
- Disclose, without authorization, any sensitive, classified, or compartmented USDA information that I access or learn as a result of my privileged user duties and activities.

Introduction & Rules of Behavior

Rules of Behavior Acknowledgement

I understand that being allowed to forego reading the ISA mandatory training materials if I take and pass the ISA Pre-Exam does not exempt me from my responsibility to understand and comply with basic security awareness. I also understand that I must follow USDA and agency Security policies, procedures and ethical and system Rules of Behavior (RoB), at all times, and I acknowledge and accept those responsibilities.

I understand that by clicking the button below, I confirm that I have read and understand the Rules of Behavior as identified in this training and understand that this may not address all RoB contained in USDA and agency policies, procedures and system-specific rules. I further understand that completion of this training does not exempt me from my responsibility to know and follow all USDA and agency policies, and procedures for RoB at all times.

I understand that access to the USDA information systems shall be granted via the USDA-issued LincPass or AltLinc card, and that it is my responsibility to use the card to access the USDA or agency network and systems at all times and report any problems with the use of the LincPass or AltLinc to my designated LincPass/AltLinc coordinator. I also understand that I must return my LincPass card to my designated LincPass coordinator or designated person as outlined by agency policy when no longer needed.

Main Mission

Welcome

Annual Basic Information Security Awareness and Rules of Behavior Training is mandatory for all USDA employees, contractors, partners, interns, and volunteers who have or will be granted access to any USDA information system.

New employees, contractors, partners, interns, and volunteers are required to complete the awareness training prior to gaining access to USDA systems. All users must stay abreast of USDA security policies, requirements, and issues.

Users must make a conscientious effort to avert security breaches by complying with USDA and agency/staff office security policies, procedures, standards, practices, and alerts.

Users are responsible for complying with the rules of behavior and this training as part of the approval process for obtaining access to a USDA information system.

Main Mission

The Journey

Information Security Awareness is an ongoing process – **it is like a journey that we all navigate and interact with a variety of technologies while doing our jobs.** To mirror this "journey," this course has been mapped into what we call the 7 Destinations of Information Security Awareness.

Your role in taking this course is to navigate through each of these Destinations and successfully pass the related assessments.

- Destination 1: Importance of Information Systems Security
- Destination 2: Controlled Unclassified Information (CUI)
- Destination 3: Personally Identifiable Information (PII)
- Destination 4: Overall Threats
- Destination 5: Internet and Network Threats
- Destination 6: Media Devices and Mobile Security
- Destination 7: Physical Security

Your progress...
You can learn how you are progressing compared to everyone else taking the course. As you begin each Destination, you will be shown statistics to how many people are currently with you at the same Destination and how many people are ahead of you.

Let your journey begin...

1: Importance of ISS

Destination Objective(s)

The Internet has made it extremely easy to quickly obtain and transfer information. While global connectivity is very convenient, it also increases our vulnerability to outside attacks. The goals of ISS and the Rules of Behavior are to protect USDA information and information systems.

ISS and Rules of Behavior protect information from unauthorized access or modification and ensure that information systems are available to their users. This means that a secure information system maintains confidentiality, integrity, and availability.

Learning Objective(s)

After completing this lesson, you should be able to:

- Identify what Information Systems Security is and why it is important.

This lesson includes the following topics:

- History of ISS.
- Critical Infrastructure.

1: Importance of ISS

History of ISS

Fifty years ago, computer systems presented relatively simple security challenges. They were expensive, understood by only a few, and isolated in controlled facilities.

Protecting these computer systems consisted of controlling access to the computer room and clearing the small number of specialists who needed such access.

As computer systems evolved, connectivity expanded, first by remote terminals, and eventually by local and wide-area networks, or LANs and WANs.

As the size and price of computers came down, microprocessors began to appear in the workplace and homes across the world.

What was once a collection of separate systems is now best understood as a single, globally connected network. ISS now includes infrastructures neither owned nor controlled by the federal government. Because of this global connectivity, a risk to one is a risk to all.

Critical Infrastructure

Critical Infrastructure Protection, or CIP, is a national program established to protect our nation's critical infrastructures. Critical infrastructure refers to the physical and cyber-based systems essential to the minimum operations of the economy and government.

Sectors considered part of our nation's critical infrastructure include, but are not limited to:

- Information technology and telecommunications.
- Energy.
- Banking and finance.
- Transportation and Border security.
- Water and Emergency services.

Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. However, these infrastructures have become increasingly automated and interlinked. Increased connectivity creates new vulnerabilities.

1: Importance of ISS

Critical Infrastructure - Threat

Equipment failures, human error, weather, as well as physical and cyber attacks impacting one sector, could potentially impact our nation's entire critical infrastructure.

For example, if the natural gas supply is disrupted by a computer virus, and electrical power is cut, computers and communications would shut down. Roads, air traffic, and rail transportation would be impacted. Emergency services would be hampered. An entire region can be debilitated because an element critical to our infrastructure has been attacked.

CIP was established to define and implement proactive measures to protect our critical infrastructure and respond to any attacks that occur.

Public Key Infrastructure

Federal information systems identify and authenticate each user either through a smart card login or user ID and password.

The preferred method of access to information systems is through the use of public key infrastructure, or PKI, which enables your agency to issue electronic keys, called digital certificates, to authorized users.

PKI allows users to encrypt and digitally sign emails and documents.

2: CUI

Destination Objective(s)

This is an awareness tutorial to introduce you to the Controlled Unclassified Information (CUI) Program. On November 4, 2010, the President signed Executive Order 13556, "Controlled Unclassified Information" (the Order). The Order established a program to standardize the way the Executive branch handles unclassified information that requires protection in accordance with law, regulation, and/or Governmentwide policy. The Order designated the National Archives and Records Administration (NARA) as the CUI Executive Agent to implement the program. NARA designated the Director of the Information Security Oversight Office (ISOO), a NARA component, to exercise these responsibilities on its behalf.

The Federal Rule, known as the Code of Federal Regulations (32 CFR Part 2002) Controlled Unclassified Information, went into effect on November 14, 2016. It establishes the government-wide policy for agencies on designating, safeguarding, disseminating, marking, and decontrolling CUI.

Learning Objective(s)

After completing this lesson, you should be able to:

- Define CUI and its purpose
- Gain an understanding of the CUI Registry and CUI categories and subcategories
- Gain knowledge on how to mark CUI documents and emails
- Understand how to protect, store, disseminate, decontrol, and destroy CUI
- Define "spillage" with respect to ISA

This lesson includes the following topics:

- Marking CUI
- CUI Protection and Storage
- Dissemination and Decontrolling of CUI
- Destruction of CUI
- Spillage
- Policies

2: CUI

What is CUI?

- ***Controlled Unclassified Information (CUI)*** *is information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies.*

- ***CUI replaces****:*
  - *For Official Use Only (FOUO)*
  - *Sensitive Security Information (SSI)*
  - *Sensitive But Unclassified (SBU), etc.*

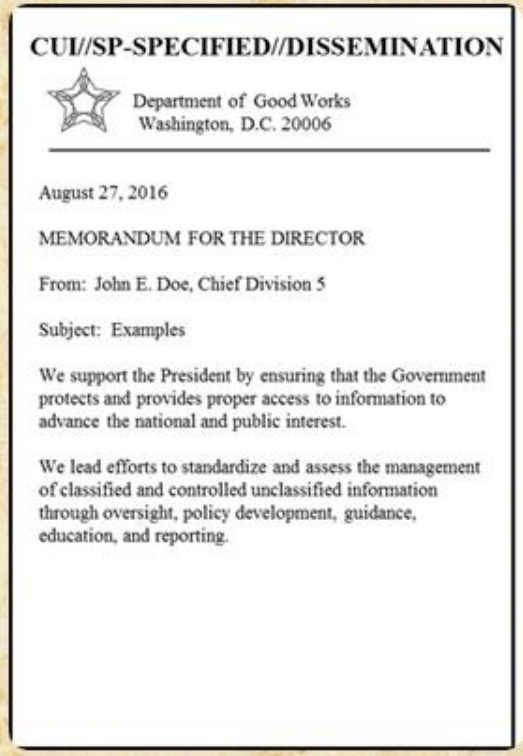
- ***The CUI Registry*** *is the repository for all information, guidance, policy, and requirements on handling CUI.*

- ***The CUI Registry****:*
  - *identifies all approved CUI categories and subcategories,*
  - *provides a brief description for each,*
  - *identifies the basis for controls, establishes markings,*
  - *and includes guidance on handling procedures.*

Marking CUI

The CUI Banner Marking may include up to three elements:

- ***The CUI Control Marking*** *(mandatory) may consist of either the word "CONTROLLED" or the acronym "CUI."*
- ***CUI Category or Subcategory Markings*** *(mandatory for CUI Specified). CUI Control Markings and Category Markings are separated by two forward slashes (//). When including multiple categories or subcategories in a Banner Marking they are separated by a single forward slash (/).*
- ***Limited Dissemination Control Markings****. CUI Control Markings and Category Markings are separated from Limited Dissemination Controls Markings by a double forward slash (//).*



CUI//SP-SPECIFIED//DISSEMINATION

Department of Good Works
Washington, D.C. 20006

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

Protection and Storage

*CUI **must** be stored or handled in controlled environments that prevent or detect unauthorized access:*

- *Sealed envelopes*
- *Areas equipped with electronic locks*

Locked:

- *Doors*
- *Overhead bins*
- *Drawers*
- *File cabinets*

Disseminating and Decontrolling

Disseminating

- Disseminating occurs when authorized holders provide access, transmit, or transfer CUI to other authorized holders through any means, whether internal or external.
- *Only the Director of Homeland Security (OHS) as the designed Senior Agency Official may approve limited dissemination controls to CUI.*

Decontrolling

- *Decontrolling occurs when an authorized holder, consistent with 32 CFR 2002 and the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action.*

2: CUI

Destruction

- ***CUI <u>must</u> be destroyed to a degree that makes the information unreadable, indecipherable, and irrecoverable.***
- ***To destroy CUI, use cross cut shredders to produce particles that are 1mm by 5 mm.***

NOT APPROVED

APPROVED

Destruction

- ***Never*** *use trash cans or recycling bins to dispose of CUI*

Spillage

Spillage, also referred to as contamination, is when information of a higher classification level is introduced to a network at a lower classification level. It is the improper storage, transmission, or processing of classified information on an unclassified system.

An example would be when information classified as Secret is introduced to an unclassified network. Any user who identifies or suspects that a spillage has occurred should immediately notify his or her security point of contact.

Cleaning up after a spillage is a resource intensive process. It can take roughly three weeks to contain and clean an affected information system. Be aware that spillages can greatly impact the security of federal information.

Helpful hints:

- Check all emails for possible classified information.
- Mark and store all removable media properly.

National and Agency CUI Policies

- *Executive Order (EO) 13556, Controlled Unclassified Information*
- *32 CFR Part 2002, Controlled Unclassified Information*
- *DM3440-001, USDA Classified National Security and Controlled Unclassified Information Program Manual*
- *DR3440-001, USDA Classified National Security and Controlled Unclassified Information Program Regulation*

Your Responsibility

Information is a critical asset to the U.S. government. It is your responsibility to protect government sensitive and classified information that has been entrusted to you.

Please contact your security point of contact for more information about classification or handling of information.

2: CUI

You are about to leave Destination 2 - Congratulations!

Once again - before you move on:

Please click (or tap if using a mobile device) the items below to acknowledge your understanding of the learning objectives of this Destination:

- √ **Define CUI and its purpose**
- √ **Gain an understanding of the CUI Registry and CUI categories and subcategories**
- √ **Gain knowledge on how to mark CUI documents and emails**
- √ **Understand how to protect, store, disseminate, decontrol, and destroy CUI**
- √ **Define "spillage" with respect to ISA**

3: PII

Destination Objective(s)

Personally Identifiable Information (PII) is a valuable and marketable commodity. Make sure it is always under your control. Otherwise ensure that it is locked up.

Encrypt it if you save it in a shared folder or on SharePoint. And, if you are sending it via email, be sure it is encrypted and is sent to others who have a job-specific reason to have it. Send the password in another email. USDA counts on you to be a PII protector and enforcer of good privacy habits.

Learning Objectives

After completing this lesson, you should be able to:

- Identify Personally Identifiable Information (PII)
- Understand your responsibility regarding PII
- Know how to respond to an "Incident" or "Breach"

This lesson includes the following topics:

- Definition of PII
- PII Responsibilities
- PII Standards
- How to handle an "Incident" or "Breach"

3: PII

What is Personally Identifiable Information (PII)?

According to NIST SP 800-122, PII is:

"Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

- PII comes in various forms: hardcopy and electronic

Examples of PII that are also perceived as PII as linkable information (this list is not all inclusive):

- Name
- Social Security Number/Tax Identification Number
- Personal Residential address
- Personal Email address
- Personal Telephone Number
- Date of Birth/Place of Birth
- Driver's License number
- Photographic image
- Fingerprints
- Voice signature
- Retina scan

If you still are uncertain about what PII is, please check with your agency's Privacy Officer/Analyst/ISSPM.

Everyone is responsible for PII at USDA

What Federal guidance makes it necessary for federal agencies to protect an individual's private info?

- The Privacy Act of 1974 as amended, 5 U.S.C. § 552a - LINK
- Office of Management and Budget (OMB) Circular A-130 - LINK
- OMB M 03-22 - LINK
- OMB M 06-16
- OMB M 17-12 - LINK
- E-Government Act of 2002 - LINK
- Fair Information Practice Principles - LINK
- Children's Online Privacy Protection Act of 1998 - LINK
- National Institute Standards and Technology Special Publication 800-122. - LINK

Standards and industry best practices

The following are some best practices when dealing with PII:

- Data minimization – privacy control – "need-to-know" and not use Social Security Number (SSN) strictly as unique identifier.
- Encrypting data in transmission and at rest.
- Protect the information as if it's your own --- deterrence to identify theft.

Secure PII - physically and logically by:

- Encrypt media devices.
- Password protect documents and separate password via separate transmission.
- Mask PII
- Don't leave PII unattended
- Use secure telephone line
- Double wrap packages

Did you know?

The Privacy Act of 1974, as amended:

Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. This act does not apply to records maintained by state, local governments, private companies or organizations. Only U.S. citizens and lawfully admitted aliens are given rights under the Act.

- Protect individual's information
- Minimize collection
- Maintain accuracy
- Identify use for records
- Specific exceptions (12) for disclosure
- Specific exemptions (10)
- Individual can request access to their record
- Individual can amend their record
- Federal agencies have administrative and physical security to prevent unauthorized release of personal records

Did you know?

Criminal Penalties

- "Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000." 5 U.S.C. § 552a(i)(1).
- "Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000." 5 U.S.C. § 552a(i)(2).
- "Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000." 5 U.S.C. § 552a(i)(3).

Did you also know?

OMB Memorandum 17-12, "Preparing for and Responding to a Breach of PII":

Definition of an **Incident:**

An occurrence that

a) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system;

or

b) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Definition of a **Breach:**

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where

a) a person other than an authorized user accesses or potentially accesses personally identifiable information

or

b) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

What do you do if you encounter a PII incident or breach?

Step 1 - Call Information Security Center (ISC) – Computer Incident Response Team via Hotline Number shown below

Step 2 - ISC conducts initial Risk Assessment AND assigns a level to the incident

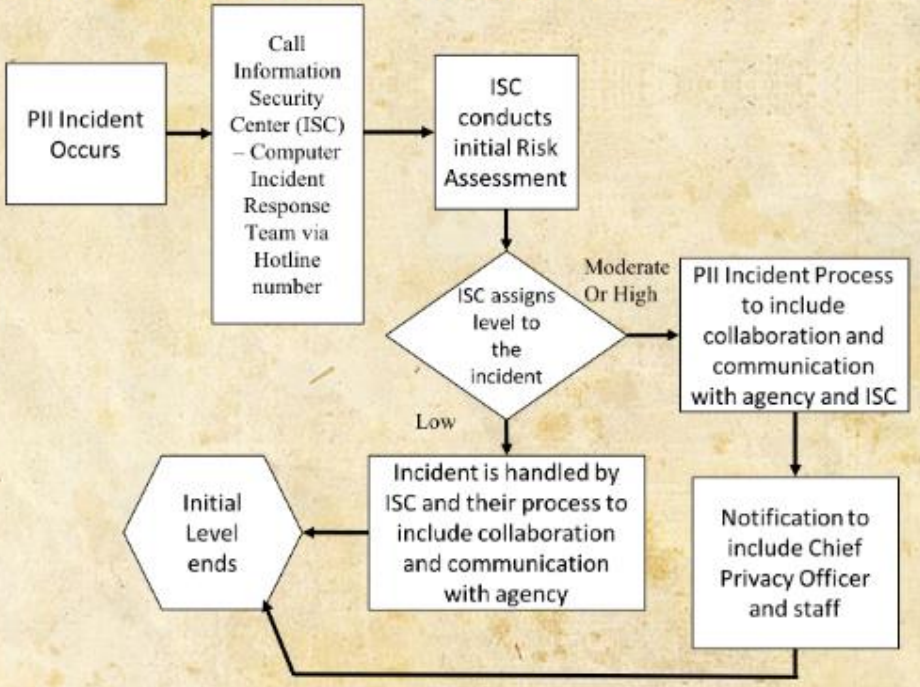
If **Low** Level Incident:

- Incident is handled by ISC and their process to include collaboration and communication with agency and Initial Level ends.

If a **Moderate** or **High** Level:

- PII Incident Process to include collaboration and communication with agency and ISC
- Notification to include Chief Privacy Officer and staff

HOTLINE NUMBER FOR PII INCIDENTS: 1-877 PII 2YOU (1-877-744-2968)



3: PII

You are about to leave Destination 3 - Congratulations!

Once again - before you move on:

Please click (or tap if using a mobile device) the items below to acknowledge your understanding of the learning objective of this Destination:

√**Identify Personally Identifiable Information (PII)**

√**PII Responsibilities**

√**PII Standards**

√**How to handle an "Incident" or "Breach"**

4: Overall Threats

Destination Objective(s)

It is important to understand the difference between threats and vulnerabilities and how they can affect your system.

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. Vulnerabilities are frequently the result of a flaw in the coding of software. To correct a vulnerability, a vendor would issue a fix in the form of a patch to the software.

Learning Objective

After completing this lesson, you should be able to:

- Differentiate between a threat and vulnerability, and identify the risks associated with each.
- Understand the differences between Internal vs. External Human Threats.

This lesson includes the following topics:

- Threat Categories.
- Environmental Threats.
- Internal vs. External Human Threats.

4: Overall Threats

Environmental Threats

Natural environmental events - including lightning, fires, hurricanes, tornadoes, or floods - pose threats to your system and information.

A system's environment - including poor building wiring or insufficient cooling for the systems - can also cause harm to information systems.

How can you protect against environmental threats?

Users should do their best to protect computer equipment from damage, abuse, theft, and unauthorized use. Users shall protect computer equipment from hazards such as:

- Extreme temperatures.
- Electrical storms.
- Water and fire.
- Static electricity.
- Spills from food and drink.
- Dropped objects.
- Excessively dusty environments.
- Combustible materials.

4: Overall Threats

Internal vs. External Human Threats

Internal

An internal human threat is a person operating within our organization. An internal threat can be a malicious or disgruntled user in the employ of terrorist groups or foreign countries or a negligent user, who inflicts unintentional damage accidentally or through a bad habit.

Let's look more closely at human threats to federal information systems. **The greatest threats to federal information systems are internal** - from people who have working knowledge of, and access to, their organization's information and computing resources.

An internal threat, or insider, is any person with legitimate physical or administrative access to the asset who can misuse or exploit weaknesses in the system.

Although there are security programs to prevent unauthorized access to information systems, and employees undergo background investigations, certain life experiences can alter people's normal behavior and cause them to act illegally. Stress, divorce, financial problems, or frustrations with co-workers or the organization are some examples of what might turn a trusted user into an insider threat.

Others, due to a lack of training and awareness, can also cause damage. This is often demonstrated through poor cybersecurity habits, such as falling victim to phishing emails or phone-based scams. By not properly evaluating a phishing email and clicking a link or opening an attached document, an internal user can cripple the entire organization's network.

How can you protect against internal human threats?

- Keep an inventory of all equipment assigned to you.
- Only use equipment for which you have been granted authorization.
- Do not leave computer equipment in a parked car or in an unsecured location where it might be stolen.
- Follow established procedures when removing equipment from USDA premises. This usually requires a property pass.
- Do not install or use unauthorized software or hardware on the network, including personal laptop computers, pocket computers, or personal digital assistants and network enabled cellular phones, except as expressly authorized.
- Do Not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Notify management before relocating computing resources.
- When possible, use physical locking devices for laptop computers and exercise additional care for other portable devices.

4: Overall Threats

Internal vs. External Human Threats

External

An external human threat is someone outside (i.e. does not have authorized access to) our organization. An external threat can be a hacker, terrorist group, foreign country, or a protester.

Within the context of information security, external human threats are often represented as hackers; however, this is an oversimplification given that external human threats have a wide variety of aims and intentions. While a cybercriminal may not desire harm to our organization and is merely seeking to exploit resources for financial gain (e.g. crypto miners), such action still has a debilitating effect on an organization. However, sophisticated, nation state-attributed actors may seek to intentionally cause harm to our organization and its overarching network.

What you should know.

- Malicious actors may include representatives of foreign countries, terrorist groups, and/or criminal elements.
- Today's hacker is also far more advanced in computer skills and has access to hacking software that provides the capability to quickly and easily identify a system's security weaknesses.
- Using tools available on the Internet, a cyber operator/hacker is capable of running automated attack applications against thousands of host computers at a time. Because of this, hackers pose a serious risk to the security of federal information systems.

4: Overall Threats

Destination 4: Done!

Once again - Before you move on:

Please click (or tap if using a mobile device) the items below to acknowledge your understanding of the learning objectives of this Destination:

√ Differentiate between a threat and vulnerability, and identify the risks associated with each.

√ Understand the differences between Internal vs. External Human Threats.

5: Internet & Network Threats

Destination Objectives:

Any network facilitates communication between individuals.

A network can be everything from a small collection of devices at a given location to the global Internet. In either case, any network is often a target for malicious intent.

By its sheer size, the Internet is the source of innumerable threats against the Department.

Learning Objectives

After completing this lesson, you should be able to:

- Understand eight (8) threats to ISA associated with networks and the Internet.
- Be able to identify three (3) or more peer-to-peer threats.
- Understand the definition of social engineering.
- Understand the definition of phishing.

This lesson includes the following topics:

- Cookies.
- Mobile Code.
- Peer-to-peer and File Sharing Software.
- General Software.
- Malicious Code.
- Internet of Things MaliciousSoftware (Malware).
- Email and Attachments.
- Hoaxes.
- Social engineering.
- Phishing.

Cookies

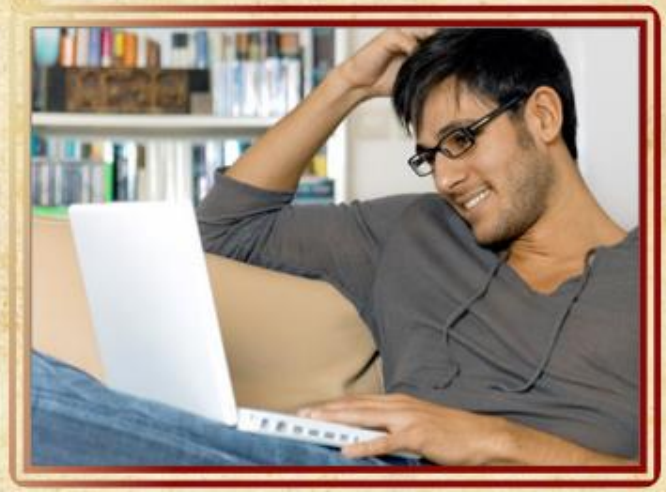
There are several security risks associated with browsing the Internet. One common risk is known as cookies.

A cookie is a text file that a web server stores on your hard drive when you visit a website. The web server retrieves the cookie whenever you revisit that website. When you return, the cookie recognizes you, saving you the trouble of re-registering.

The most serious security problem with cookies has occurred when the cookie has 'saved' unencrypted personal information, such as credit card numbers or Social Security numbers, to facilitate future business with that site. Another problem with cookies is that the site can potentially track your activities on the web.

To reduce the risk associated with cookies, and better protect your system, your browser should be set up to not accept cookies.

Mobile Code



Mike wants to see a funny website his friend told him about, but first he must load and run an application to see the website. If Mike runs the application, he may be vulnerable to malicious mobile code.

Mobile code, such as ActiveX and Java, are scripting languages used for Internet applications.

Mobile code embedded in a web page can recognize and respond to user events such as mouse clicks, form input, and page navigation. It can also play audio clips.

However, it does introduce some security risks. Mobile code can automatically run hostile programs on your computer without your knowledge simply because you visited a web site. The downloaded program could try to access or damage the data on your machine or insert a virus.

Review your agency's policies for specific guidance or restrictions on the use of mobile code.

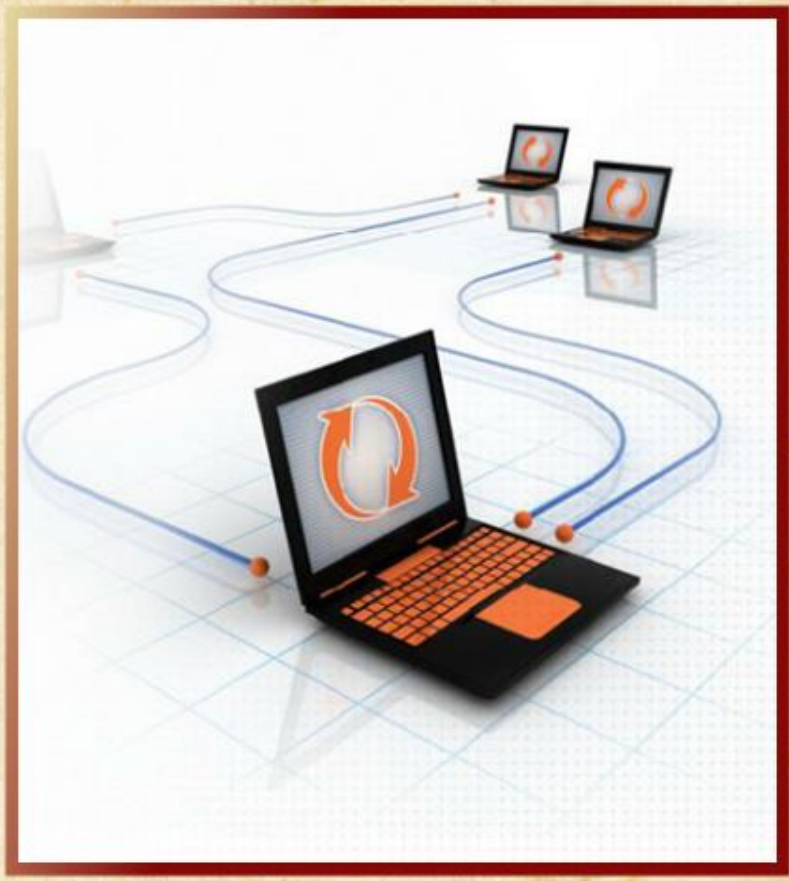
Peer-to-Peer (P2P)

Peer-to-peer (P2P) file sharing technology is a way to share files, play games, and facilitate online telephone conversations.

The technology enables computers using the same or compatible P2P programs to form a network and share files directly with other computers in a network.

P2P file sharing programs allow people to download files and make them available to other users on the network.

P2P users can designate the drives and folders from which files can be shared. In turn, other users can download and view any files stored in these designated areas.



File sync and sharing

Cloud-based file syncing and sharing services implement automated file transfers by updating files from a dedicated sharing directory on each user's networked devices.

Files placed in this folder also are typically accessible through a website and mobile app, and can be easily shared with other users for viewing or collaboration.

Such services have become popular via consumer-oriented file hosting services such as Dropbox and Google Drive.

P2P Vulnerabilities

People who use P2P file sharing software can inadvertently share files. They might accidentally choose to share drives or folders that contain sensitive information, or they could save a private file to a shared drive or folder by mistake, making that private file available to others.

In addition, viruses and other malware can change the drives or folders designated for sharing, putting private files at risk.
Peer-to-peer connections are a common avenue for the spread
of computer viruses and spyware.

Obtaining copyrighted files at no cost raises not only ethical concerns, but could result in criminal or civil liability.

The installation and use of unauthorized peer-to-peer applications can also result in significant vulnerabilities to your agency's networks, including exposure to unauthorized access of information and compromise of network configurations.

The following list provides examples of some P2P software divided by category:

Instant Messaging / Telephony:

- iMessage
- QQ
- Line
- eBuddy
- Windows Live Messenger

File Sharing:

- BitTorrent
- Gnutella
- Kazaa
- WinMX
- Napster
- PC Anywhere
- eDonkey
- Morpheus
- eMule
- LimeWire
- BearShare
- Timbuktu

About P2P File Sharing

As a reminder:

- Users are prohibited from using peer-to-peer (P2P) file sharing unless specifically approved by management in writing.
- The Office of Management and Budget (OMB) requires all Agencies to develop guidance on the use of peer-to-peer applications.
- Contact your security point of contact for further information on your specific policy regarding the use of peer-to-peer applications.

Internet of Things

The Internet of Things (IoT) is the concept of connecting any device with an on/off switch to the Internet, especially those devices which historically were not used for computing. This includes everything from household items (e.g. thermostats, washing machines, lamps, coffee makers) to automobiles, even to medical devices (e.g. pacemakers). While this type of interconnection provides a great deal of automation and end-user convenience, it also presents a huge opportunity for exploitation. Frequently, IoT devices that have not before been used for computing are not designed with security in-mind or, if they are, designers have difficulty in envisioning how hackers may exploit them. Thus, any vulnerable IoT device increases the attack surface.

IoT devices are likewise being used in agriculture to include environmental controls and harvesting equipment. For example, harvesters frequently use navigation equipment, the disruption of which, could have debilitating consequences. For further information regarding this topic, please see Threats to Precision Agriculture.

Learning Objective

After completing this lesson, you should be able to:

- Identify the threat posed by malware and identify how to protect federal information systems from malicious code.

This lesson includes the following topics:

- Email and Attachments.
- Hoaxes.

Malware

Malware is short for "malicious software". Malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include:

- Viruses – Malware that generally needs user interaction to execute; once executed, it replicates itself and modifies other legitimate programs for a variety of purposes.
- Worms – Malware that is self-replicating (i.e. no user interaction is required), often performing the same actions as viruses; because they are self-replicating, they are frequently more destructive.
- Trojans – Malware that frequently appears legitimate, which tricks users to installing it on their devices. Once activated, it allows an attacker to execute several actions on a system, including information stealing/credential harvesting and creating backdoors, thereby giving an attacker direct access to a system.

Malware is specifically designed to disrupt, damage, or gain unauthorized access to a computing system (e.g. desktop, laptop, tablet, mobile phone). That said, malware applications are used for a variety of purposes, the most common of which, are monetary in nature. Examples of monetary-based malware include:

- Ransomware –prevents users from access data until a ransom is paid
- Cryptomining – allows an attacker to use a victim's system to mine for cryptocurrency
- Banking Trojan – harvests confidential information related to banking and payment systems

The most common method for the delivery and distribution of malware is email-based phishing, which entices a user to click a link or open an attachment. However, there are other delivery methods, including baiting (i.e. dropping an infected USB drive outside of an office, hoping an employee connects it to a system resource) and water hole attacks (i.e. compromising a legitimate website to infect those who visit the website).

Email and Attachments

Email messages and email attachments provide a common route to malware.

Always be cautious when opening email attachments – they may contain malicious code that could corrupt files, erase your hard drive, or enable a hacker to gain access to your computer.

Files to be cautious of include: .html, .pdf, .url, .doc(x), .xls(x), or .rtf and any file extension that the sender asks you to change to a different extension (i.e. .xxx to.exe). USDA quarantines all files with these extensions, plus more.

While specific file types are quarantined, prevention is never 100% attainable. As an example, Emotet is one of the most prolific banking trojans seen in recent years; while its historic focus was financial gain, it can be used to deliver a variety of other malicious payloads as well as steal a great deal of non-banking related information. During FY18, USDA experienced 56 Emotet compromises; each of these was caused by a USDA employee or contractor falling victim to a phishing email. While we don't have specific numbers for beyond FY18 at this time, it appears that there has been an increase.

Don't assume that an attachment is safe because a friend or coworker sent it. Some malware is activated by merely opening the message. Save the attachment to your hard drive and scan it with up-to-date anti-virus/anti-malware software before opening it. If you require assistance with this, please contact your agency's IT support center.

Never click on suspicious links in email messages, even if it appears to be from someone you are familiar with. If you suspect an email message to be a phishing attempt, please notify spam.abuse@usda.gov.

What you should know.

Protect Your Computer System

- Scan email attachments and outside files using anti-virus software that has current updates.
- Ensure system is scanned daily.
- Delete email from unknown or unexpected sources.
- Turn off email software option to automatically download attachments.

Respond to a Malware Attack

- Do not email a copy of the infected file.
- Contact your agency help desk or security contact.

Hoaxes

An email Phyllis gets from a good friend includes a warning about a serious computer virus. Her friend says to tell everyone she knows. If Phyllis forwards the email to her office email group, is she helping or promoting an "Internet Hoax?"

Internet hoaxes are email messages designed to influence you to forward them to everyone you know.

Hoaxes encourage you to forward email messages by warning of new viruses, promoting moneymaking schemes, or citing a fictitious cause. By encouraging mass distribution, hoaxes clog networks and slow down Internet and email service for computer users.

If you receive an email message requesting that you forward it to all your friends and coworkers, do not forward the email.

Social Engineering

When Kate answered the phone, the man on the other end sounded very authoritative. He said he was investigating a possible security incident on USDA's WebTA time and attendance information system and needed her to verify her password. Kate may have been the target of social engineering.

Social engineering is the use of deception to manipulate individuals or groups into revealing personal or sensitive information that may be used for fraudulent purposes. There are a variety of social engineering techniques, with phishing (email solicitation) and vishing (voice solicitation, often via phone calls) being two of the most popular.

Common social engineering tactics include, but are not limited to:

- Phishing – email solicitation that frequently attempts to entice a victim to click a link or open an attachment, which will collect information or execute a malicious payload; this will be covered in greater detail in a later section.
- Vishing – voice solicitation where an attacker speaks to a target, often over the phone, attempting to collect information.
- Quid Pro Quo – receiving a benefit/something in exchange for information (e.g. "I'm from tech support and need to fix something on your system; what's your password?")
- Baiting – leaving USB drives or optical media in a conspicuous area, hoping that a potential target will "discover" the item and plug it into a network device.
- Tailgating – Gaining access to the network under someone else's ID (e.g. "Can I use/check something on your computer for a second?")

Nobody should ever ask you for your passwords. This includes system administrators and help desk personnel.

Your Role in Social Engineering

Understanding social engineering behaviors will enable you to recognize them and avoid providing important security information to unauthorized sources.

Preventing social engineering:

- Verify identity.
- Do not give out passwords.
- Do not give out employee information.
- Do not follow commands from unverified sources.
- Do not distribute dial-in phone numbers to any computer system except to valid users.
- Do not participate in telephone surveys.

Reacting to social engineering:

- Use Caller ID to document phone number.
- Take detailed notes.
- Get person's name/position.
- Report incidents.

Phishing

Linda received an email from her bank that her debit card account may be at risk, and she needs to verify her account and PIN numbers. **Is someone "phishing" for Linda's private information?**

Phishing is the fraudulent practice of sending emails (or other messages) purporting to be from actual, reputable organizations in order to trick the target individuals to either reveal sensitive information or to install a malicious application. Phishing is the most common form of social engineering and typically attempts to entice the targeted individual(s) to reply directly with information, click on a link, or open an attachment.

When links are clicked or attachments are opened, malware is frequently installed, enabling the attacker access to a system. Or, when links are clicked, targeted individuals are directed to a website that appears legitimate, where they are tricked into entering sensitive information (e.g. passwords).

In addition to emails, phishers use text messages, social media communication, and pop-up messages. All of these generally have the same intent: trick the user into either revealing information or installing a malicious application.

Phishing (continued)

Phishers send an email or pop-up message that claims to be from a business or organization that a user deals with. For example, phishers often pose as a user's Internet online payment service, or even a government agency.

- The message usually says that the user needs to update or validate account information and may threaten some dire consequence if the user does not respond.
- The message directs the user to a website that looks just like a legitimate site, but it is not affiliated with the organization in any way.
- The purpose of the bogus site is to trick the user into divulging personal information so the operators can steal the user's identity and run up bills or commit crimes in the user's name.
- The bogus site may also install malicious code on the user's system.

Phishing Examples

If you receive an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message.

Legitimate companies do not ask for this information via email. If you are concerned about your account, contact the organization identified in the email using a telephone number you know to be genuine. Be cautious if you receive an email regarding any financial transaction containing links to obtain more information or dispute a charge, even from vendors you regularly receive email from. Always hover over these links to make sure they go to a valid domain associated with this business. Do not click if you have any suspicions about a link. Ask for verification from this business via a good email address or their web portal.

While attackers are generally good about masking weblinks, often times a close inspection reveals malicious links.

Sample domains:

Valid — https://www.amazon.com/gp/pdp/profile/...

Suspicious — http:// www.amazon.com.suspicious.me/wp-...

Suspicious — http://suspicious.me/www.amazon.com/e4f6d23...

Phishing Examples (continued)

As previously stated, weblinks may be masked (i.e. the hyperlink appears to the user as https://www.amazon.com, but clicking on it takes the user to an attacker's site). Thus, weblinks should not be taken as indicators in and of themselves but rather as a data point that the user needs to evaluate within the entire context of the message. In other words, the user should consider whether or not the message was expected, who the message is from, the link involved, message content/verbiage, spelling/grammar, and tone. If you suspect that a message is a phishing attempt, please forward it to spam.abuse@usda.gov.

- In recent years, U.S. Government email recipients have received messages from external individuals in the same field of business. The phishing messages were sent via well-known file delivery services like Dropbox.com, Box.com, or Yousendit.com. The files available for download contained malicious code. If these files were opened, they would install remote access software that permitted external organizations access to U.S. Government files and systems. While this demonstrates how a phishing scheme can work, it also shows how publicly-available cloud storage services can be used for malicious purposes and reinforces why file drop services should never be used to store or transmit proprietary USDA information.

5: Internet & Network Threats

You're more than halfway through your adventure!

Once again - Before you move on:

Please click (or tap if using a mobile device) the items below to acknowledge your understanding of the learning objectives of this Destination:

- √ **Understand eight (8) threats to ISA associated with networks and the Internet**
- √ **Be able to identify three (3) or more Peer-to-Peer threats.**
- √ **Understand the definition of Social Engineering**
- √ **Understand the definition of Phishing**

6: Media Devices and Mobile Security

Destination Objectives

Threats to information security come from a variety of sources. This destination discusses threats from devices such as thumb drives, cell phones, smart phones, and wireless networks.

In addition to discussing the threats, this Destination provides tips on keeping your mobile device secure and what you should do if you lose your phone.

Learning Objectives

After completing this lesson, you should be able to:

- Understand the threats to ISA from areas such as media devices (e.g. thumb drives), mobile devices, and wireless networks.
- Know what to do if you lose your cellphone with respect to ISA.

This lesson includes the following topics:

- Media Devices.
- Cellular (dumb) and Smart Phones.
- Mobile Device Security.
- Laptops and Fax Machines.
- Wireless Networks.

Media Devices

Be extremely careful when using cell phones, smart phones, laptop and tablet computers, fax machines, and wireless networks. You need to be as vigilant about security on these devices as you are with your computer at work.

Cell (Dumb) Phones, Smart Phones & Mobile Devices

If you use a cell phone, anyone with the right equipment could potentially listen to your conversation. Cell phones are merely transmitters.

Use a landline for more privacy, and never discuss sensitive information on an unsecured phone.

Smart Phones pose an additional security threat for several reasons.

Their small size and relatively low cost make them easy to obtain and difficult to control.

All Smart Phones connecting to government systems should be in compliance with your agency's policy and Federal guidance.

Mobile Device Security Basics

Smart Phones and Tablets are Handheld Computers NOT Cell Phones

Today, mobile devices have many of the same features as traditional computers; they also face many of the same threats. To keep your mobile device secure, you should follow computer security best practices.

For example:

- To prevent unauthorized access to your phone or tablet, set a personal identification number (PIN) or password.
- Turn off networking (e.g., Bluetooth) and tracking (e.g., GPS) features when not needed.
- Do not open unsolicited email messages.
- Don't follow links in unsolicited email messages or open attachments.
- Do not open or follow links in unsolicited text messages.
- Do not store sensitive emails, photos or documents on your mobile device.
- Keep your mobile device updated and patched to the latest revisions.
- Backup and secure your data frequently.

Mobile Device Security Basics

Don't Jailbreak any Mobile Device

Mobile devices should be treated like computers; however, there is one major way that a mobile device differs from a computer that requires special attention – smart phones and tablets can be jailbroken.

Unlocking, or Jailbreaking, a smart phone removes built-in security protections that protect the device from malicious applications.

What you should know.

- It is very important that you don't modify your smart phone's security settings for convenience. Tampering with a smart phone's factory settings, jailbreaking, or rooting a USDA smart phone undermines the built-in security features offered by USDA, the wireless service provider, and the smart phone manufacturer, while making it more susceptible to unauthorized access.

Mobile Device Security Basics

Use Caution When Downloading Applications

Mobile devices can be quickly customized with a range of applications. Unfortunately, downloading new applications can sometimes be too easy. Malicious applications can cause performance issues, compromise the confidentiality or integrity of USDA information that you do not intend for the applications to have, or even take control of the device.

Use the following tips when selecting and installing applications for USDA mobile devices:

- Only download applications from vendor's approved application store when authorized.
- Don't be afraid to choose "Don't Allow" when configuring new applications. If an application is asking for access to information or capabilities like GPS tracking on a mobile device that does not seem related to its intended use, choose the "Don't Allow" option when prompted.

Mobile Device Security Basics

Keep Your USDA Mobile Devices Physically Secure

Because mobile devices are commonly lost or stolen, it's important to secure and keep track of them. If someone picks up your mobile device, they may try to use it to access your account or information.

To help keep your mobile device physically secure, follow US-CERT's tips:

http://www.us-cert.gov/cas/tips/ST04-017.html - LINK

Mobile Device Security Basics

Immediately Report a Lost or Stolen Mobile Device

If a USDA mobile device is lost or stolen, you should report it immediately. Lost or stolen USDA devices should be reported to:

- The 24-hour stolen equipment hotline (888-926-2373).
- The local authorities (if stolen).
- Any other personnel required by your agency's chain of command.

After a mobile device is reported as lost, USDA will make sure that the device is turned off and electronically wiped clean. This prevents an unauthorized person from using the found or stolen device to access USDA resources.

While the cost of the replacement mobile device is minimal, the loss or exposure of USDA data is priceless.

Mobile Device Security Basics

Backup Your Mobile Device Regularly

Information stored locally on the mobile device cannot be recovered if you do not manually backup your mobile device. Contact your agency Help Desk for instructions on how to backup your mobile devices.

Backups are quick and easy – create a backup routine that is easy to remember and follow.

Learn More!

Run through the Smartphone Security Checker, an online tool to help consumers secure mobile devices, by visiting the site and selecting the mobile operating system.

What you should know.

The tool will provide 10 customized steps and tips to protect the device.

Laptops & Fax Machines

The convenience of laptops and notebook computers makes them extremely vulnerable to theft or security breaches.

User logon information should always be password protected.

Be careful what you display on the screen when it is visible to others, especially in close quarters, such as on airplanes.

Maintain possession of the laptop at all times when traveling. When you reach your destination, be sure that the laptop is properly secured when left unattended. If the laptop has wireless capability, ensure that security features are properly configured in accordance with your agency's wireless policy. When not in use, laptop wireless should be turned "off" or, if this is not possible, it should be configured to connect to recognized Internet access points, not ad hoc networks.

An Office of Management and Budget (OMB) memorandum states: All sensitive data stored on laptops should be encrypted. Ensure that you follow both your agency's and OMB's guidance on encryption of sensitive data on laptops.

When transmitting sensitive information over a fax machine, ensure that the recipient will be present to pick up the fax immediately. Contact the recipient directly to confirm receipt of the fax. Never transmit classified information via an unsecured fax machine.

Always use a cover sheet so that the content of your fax isn't immediately visible.

Wireless Networks

As a reminder:

- Wireless networks operate by using radio signals, instead of traditional computer cables, to transmit and receive data.
- Unauthorized users with a receiver can intercept your communications and access your network.
- This is dangerous because unauthorized users may be able to capture not only the data you are transmitting, but also any data stored on your network.

6: Media Devices and Mobile Security

Destination 6: Done!

Once again - Before you move on:

Please click (or tap if using a mobile device) the items below to acknowledge your understanding of the learning objectives of this Destination:

✓ **Understand the threats to ISA from areas such as media devices, mobile devices, wireless networks.**

✓ **Know what to do if you lose your cellphone with respect to ISA.**

7: Physical Security

Destination Objectives

This Destination focuses on physical security related to Information Security. Physical security is the first line of defense of information security and consists of everything from how you access your work environment to protecting your passwords to keeping track of what equipment has been issued to you.

Learning Objective(s)

After completing this lesson, you should be able to:

- Recognize what makes up physical security of information systems
- Understand effective password creation and management

This lesson includes the following topics:

- Physical Security Essentials.
- Inventory Control.

Physical Security

Protecting federal information systems and the information they contain starts with physical security. Physical security includes protection of the entire facility, from the outside perimeter to the offices inside the building, including all the information systems and infrastructure.

You are responsible for knowing your organization's physical security policies and following them. Your organization should have procedures for gaining entry, procedures for securing your work area at night, and emergency procedures.

These may include:

- The use of a badge or key code for entry.
- Locking your cubicle.
- Undocking your laptop and storing it in a separate location.
- Securing data storage devices, such as hard drives and USB drives during emergency procedures.

Physical Security – Proactive Approach

You should also make sure others follow your organization's physical security policies and challenge people who don't. Don't allow people to gain entrance to a building or office by following someone else instead of using their own badge or key code.

Challenge people who do not display badges or passes. If you are the last person to leave in the evening, make sure that others have secured their equipment properly.

Finally, you are responsible for reporting any suspicious activity that you see.

Inventory Control

Part of physical security includes controlling the inventory of equipment that stores federal information. When government laptops are lost or stolen, so is the information that is on them. In recent years, federal inventory control procedures have been tightened in response to the loss of thousands of government laptop computers.

Federal agencies are responsible for controlling their inventory of office and computer equipment, including phones, computers, printers, faxes, monitors, and USB drives.

When you receive government property, you should sign for it. Once it has been signed out to you, you are then responsible for that equipment and taking the necessary precautions to ensure that it doesn't get lost or stolen.

To remove equipment from the building, or bring equipment into the building, your organization may require you to have a property pass signed by the property manager.

If that property is lost or stolen, follow your organization's procedures for reporting the loss. In addition to reporting the loss of the equipment itself, you must report the loss of the information that was on the equipment and the significance of that lost information.

Telework Procedures

Telework, also known as telecommuting, is emerging as a viable option for employees. Advances in computer and telecommunications capabilities make telework increasingly practical.

There are risks associated with remote access to your government computer network.

If you have received approval for teleworking, you are required to satisfy the requirements in your agency's policies and guidelines.

7: Physical Security

You have sailed through Destination 7!

Once again - Before you move on:

Please click (or tap if using a mobile device) the items below to acknowledge your understanding of the learning objectives of this Destination:

√**Recognize what makes up physical security of information systems**

√**Understand effective password creation and management**

Finish Line!

Final Exam Time

You have navigated through all 7 Destinations!

Now, you should be prepared for the final exam for the USDA Information Security Awareness Training.

There are 14 questions in the final exam. You must achieve a score of 70% or higher to fulfill your mandatory training requirement. Once you have achieved this score, the course will be moved to your Completed Work area.

LINK to Information Security Awareness Quiz