LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

The Department of Health and Human Services Information Systems Security Awareness Training

Fiscal Year 2015

Information Systems Security Awareness

Introduction

Information Systems Security Awareness

This course is designed to provide Department of Health and Human Services (HHS) employees, contractors, and others with access to Department systems and networks with knowledge to protect information systems and sensitive data from internal and external threats.

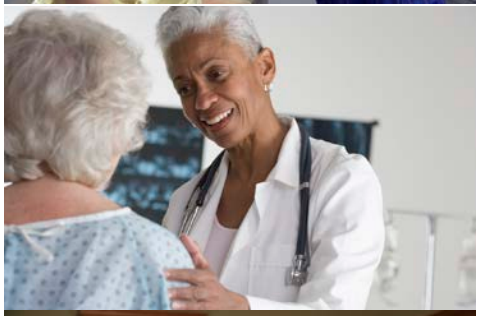
This course fulfills the Federal Information Security Management Act of 2002 (FISMA) requirement for security awareness training for users of federal information systems.

The course will take approximately 60 minutes to complete.

You will read and acknowledge the *HHS Rules of Behavior* at the end of the course.

Introduction

The HHS Mission and You



HHS employees and contractors routinely access sensitive data like names, Social Security numbers, and health records to successfully carry out HHS' mission of *"protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves."*

Introduction

HHS Personnel Are the Best Line of Defense

HHS personnel are critical to the defense and protection of sensitive Department information systems and data.

You will be well equipped to protect HHS by incorporating the information technology (IT) security objectives learned in this course into your daily work.

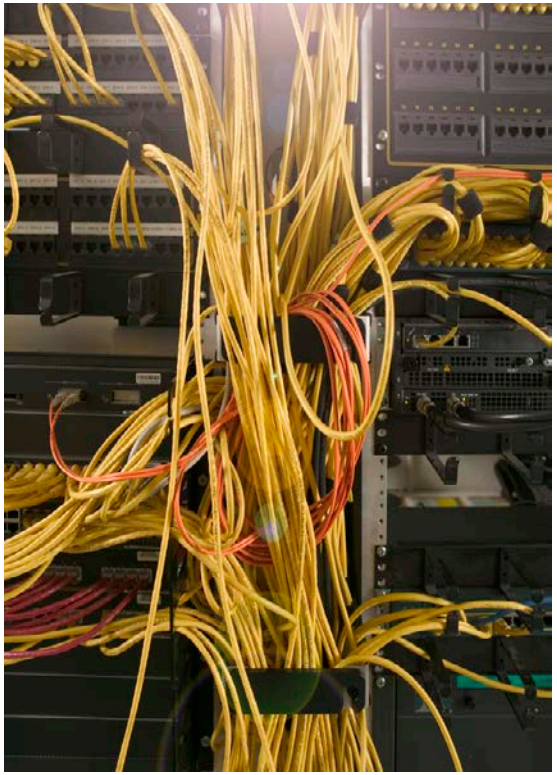
Introduction

Objectives

At the end of the course, you will be able to:

- ❑ Define information systems security;
- ❑ Identify federal regulations that mandate the protection of IT assets;
- ❑ Understand HHS' IT security policy, procedures, and practices;
- ❑ Understand personal responsibility to protect information systems;
- ❑ Recognize threats to information systems and privacy;
- ❑ Identify best practices to secure IT assets and data in and out of the office;
- ❑ Define privacy and personally identifiable information (PII); and
- ❑ Identify the correct way to respond to a suspected or confirmed security or privacy incident.

Information Security Overview



Information Security Overview

Did You Know?

- The security company, Symantec, reported targeted cyber attacks rose 42% in 2012.

Source: CNET, http://news.cnet.com/8301-1009_3-57579847-83/targeted-cyberattacks-jump-42-percent-in-2012-symantec-says/

- The Internet Crime Complaint Center (IC3) reported that consumers lost over $525 million due to Internet scams in 2012.

Source: Internet Crime Complaint Center, http://www.ic3.gov/media/annualreport/2012_ic3report.pdf

- The Federal Trade Commission (FTC) counted 369,132 complaints about identity theft in 2012, meaning the crime accounted for 18% of the 2 million total complaints the agency received. Identity theft is at the top of the consumer complaint list for the 13th year in a row.

Source: Federal Trade Commission, http://www.ftc.gov/opa/2013/02/sentineltop.shtm

Every year cyber attacks become more sophisticated and result in large losses of personal and financial data. Knowledge about how to protect information systems is vital to the effectiveness of the Department's operations and ability to accomplish our mission.

Objective
✓ Define information systems security

Information Security Overview

What is Information Security?

Information Security (IS) – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- Information security is achieved through implementing technical, management, and operational measures designed to protect the **confidentiality, integrity and availability** of information.
- The goal of an IS program is to **understand, manage, and reduce the risk to information** under the control of the organization.

In today's work environment, many information systems are electronic; however HHS has a media neutral policy towards information, meaning that any data whether in electronic, paper, or oral format must be protected.

Objective
✓ Define information systems security

Information Security Overview

Key Concepts

There are three elements to protecting information:

- **Confidentiality** – Protecting information from unauthorized disclosure to people or processes.
- **Availability** – Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users.
- **Integrity** – Assuring the reliability and accuracy of information and IT resources.

Your bank ATM is a good example of an information system that must be confidential, available, and have integrity.

- Imagine if your account was not kept **confidential** and someone else was able to access it when they approached the ATM. How much damage could be done?
- Imagine if your bank's ATM was rarely **available** when you needed it. Would you continue to use that bank?
- Imagine if every time you went to the ATM, the balance it displayed was inaccurate. How could the poor **integrity** of your balance information adversely affect your account management?

Objective
✓ Define information systems security

Information Security Overview

Key Concepts

Threats and vulnerabilities put information assets at risk.

- **Threats** – the potential to cause unauthorized disclosure, changes, or destruction to an asset.
  - Impact: potential breach in confidentiality, integrity failure and unavailability of information
  - Types: natural, environmental, and man-made
- **Vulnerabilities** – any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.
- **Risk** – the likelihood that a threat will exploit a vulnerability. For example, a system may not have a backup power source; hence, it is vulnerable to a threat, such as a thunderstorm, which creates a risk.

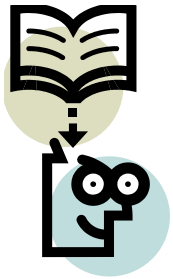
Objective

✓ Define information systems security

Information Security Overview

Key Concepts

- **Controls** – policies, procedures, and practices designed to manage risk and protect IT assets.
- Common examples of controls include:
  - Security awareness and training programs;
  - Physical security, like guards, badges, and fences; and
  - Restricting access to systems that contain sensitive information.



Knowledge Check

What is the goal of information security? *(choose the best answer)*

- A: Ensure that employee passwords contain at least eight characters.
- B: Protect the confidentiality, availability, and integrity of information and information systems.
- C: Eliminate all threats to information systems.
- D: Provide a lock for all file cabinets in the building.

Knowledge Check - Answer

The correct answer is:

The goal of information security is to protect the confidentiality, availability, and integrity of information and information systems.

Information Security Policy and Governance

Objective

✓ Identify federal regulations that mandate the protection of IT assets

Information Security Policy and Governance

Federal Government Governance

The table lists some sources of legislation and guidance that provide the backbone to governance that protects federal information and systems.

IT Security Legislation and Guidance	Privacy Legislation	National Institute of Standards and Technology (NIST) Special Publications
▸ E-Government Act of 2002 ▸ Clinger-Cohen Act of 1996 ▸ Health Insurance Portability and Accountability Act of 1996 (HIPAA) ▸ Office of Management and Budget (OMB) Circular A-130	▸ Privacy Act of 1974 ▸ Paperwork Reduction Act ▸ Children's Online Privacy Protection Act (COPPA)	▸ NIST issues standards and guidelines to assist federal agencies in implementing security and privacy regulations. ▸ Special publications can be found at: http://www.nist.gov/publication-portal.cfm.

Objective

✓ Understand HHS' IT security policy, procedures, and practices

Information Security Policy and Governance

Department Governance

- The **Department** sets programmatic direction by providing an enterprise-wide perspective, facilitating coordination among key stakeholders, setting standards and providing guidance, and supporting streamlined reporting and metrics capabilities.
- **HHS Cybersecurity Program** is the Department's information security program. Oversight is provided by the Office of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO).
- **Operating Divisions (OpDivs)** implement programs that meet specific business needs, provide business/domain expertise, manage implementation at the OpDiv level, develop policies and procedures specific to the operating environment, and manage ongoing operations.

Objective

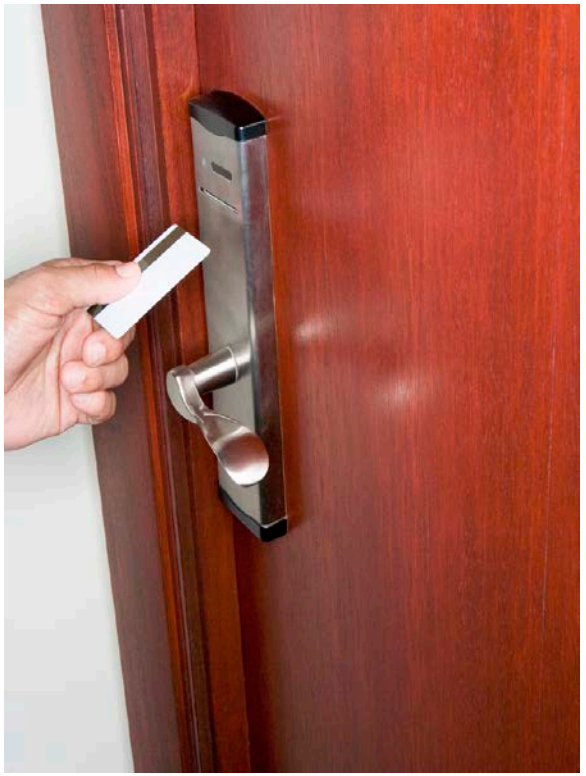
✓ Understand HHS' IT security policy, procedures, and practices

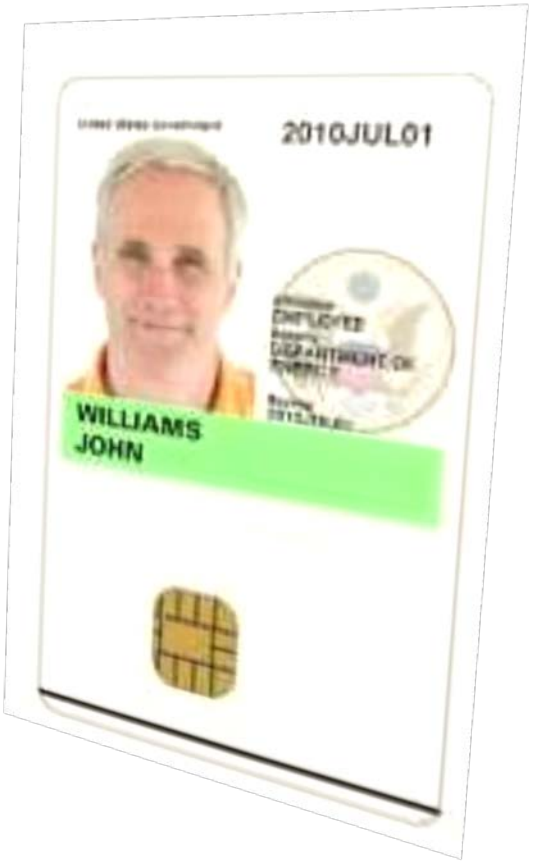
Information Security Policy and Governance

Department Governance

- The *HHS-OCIO Policy for Information Systems Security and Privacy* provides direction on developing, managing, and operating an IT security program to the OpDivs and Staff Divisions (StaffDivs).
- *Rules of Behavior For Use of HHS Information Technology Resources* sets the policies for using Department systems. Operating Divisions may have additional policies and programs specific to their operating environment, however they shall not be less strict than the Department's rules.

Physical Access Controls





Objective

✓ Identify best practices to secure IT assets and data in and out of the office

Physical Access Controls

Password Protection

- A strong password for your network account and other applications is a basic protection mechanism.
- While it is tempting to create an easy or generic password that is easy to remember, it is not very secure.
- Two rules for stronger passwords:
  - Create a password at least eight characters in length.
  - Password should contain at least one each:
    - Capital letter
    - Lowercase letter
    - Number
    - Special character (%,^,*,?)

Objective

✓ Identify best practices to secure IT assets and data in and out of the office.

Physical Access Controls

Password Protection

- Having trouble remembering passwords? Use a passphrase.
  - Use the initials of a song or phrase to create a unique password
  - Example: “Take me out to the ballgame!” becomes “Tmo2tBG!”
- Commit passwords to memory. If you are still having trouble, then write it down and keep it in a secure place, like your wallet.
- **DO NOT** keep passwords near your computer or on your desk.

Objective

✓ Identify best practices to secure IT assets and data in and out of the office.

Physical Access Controls

Password Protection Tips

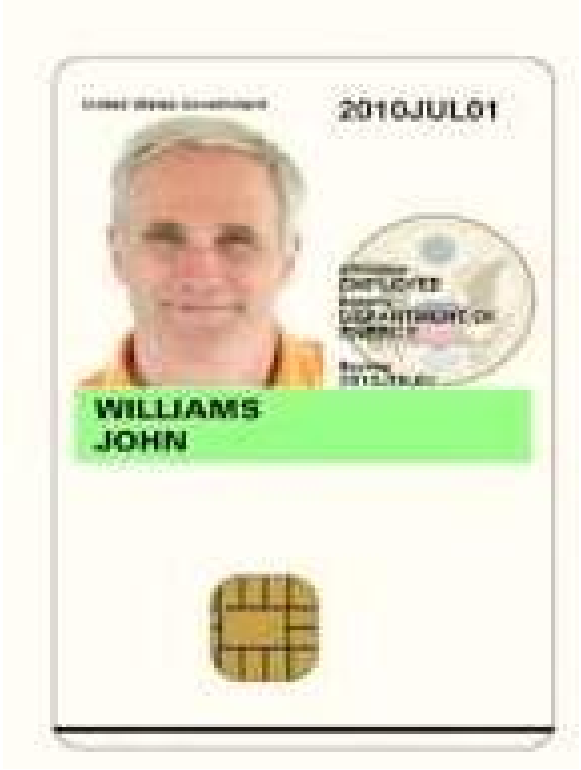
- ✓ Change password often. Most applications will remind you to do this but if not, set up a reminder in your calendar at least every 60 days.
- ✓ Change password immediately if you suspect it is compromised.
- ✓ Create a different password for each system or application.
- ✓ Do not reuse passwords until six other passwords have been used.
- ✓ Do not use generic information that can be easily obtained like family member names, pet names, birth dates, phone numbers, vehicle information, etc.
- ✓ **NEVER** share your password with anyone.

Objective

✓ Identify best practices to secure IT assets and data in and out of the office.

Physical Access Controls

Personal Identity Verification Card



- Personal Identity Verification (PIV) cards use radio frequency identification chips to reliably identify employees and contractors, and grant access to HHS buildings and government-issued computers.
- PIV cards contain PII about you and must be protected like a password.
  - Maintain possession of your PIV card at all times. Remember to remove it from your computer when you leave your workstation.
  - If your PIV card is lost or misplaced, report it to the security office immediately.
  - Keep your PIV card in a secure badge holder to shield it against unauthorized reading.

Objective

✓ Identify best practices to secure IT assets and data in and out of the office.

Physical Access Controls

Tailgating

Physical security is an important information systems safeguard. Limiting physical access to information systems and infrastructure to authorized personnel diminishes the likelihood that information will be stolen or misused.

Combat tailgating

- Never allow anyone to follow you into the building or secure area without his or her badge.
- Be aware of procedures for entering a secure area, securing your workstation when you leave the office, and securing your workstation during emergencies.
- Do not be afraid to challenge or report anyone who does not display a PIV card or visitor's badge.
- Escort visitors to and from your office and around the facility.
- Do not allow anyone else to use your PIV card for building or secure area access.
- Report any suspicious activity to the security office.

Objective

✓ Identify best practices to secure IT assets and data in and out of the office

Physical Access Controls

Physical Security Protection Tips

- ✓ Lock your computer when it is not in use.
- ✓ Remove your PIV card when leaving your workstation. Do not leave it in the card reader.
- ✓ Store and transport removable media such as CDs, DVDs, flash drives, and external hard drives in a secure manner to prevent theft or loss.
- ✓ Only connect government authorized removable media devices.
- ✓ Encrypt all devices which contain PII and sensitive information.
- ✓ Keep sensitive information out of sight when visitors are present.
- ✓ Quickly retrieve faxes that are sent to you. Always confirm that the recipient received the fax that you sent.

Physical Access Controls

Knowledge Check

Which password is most secure?

- A: linda12
- B: 123Abc
- C: Big_Apple!
- D: B&H17Plu$3428

Physical Access Controls

Knowledge Check - Answer

The correct answer is:

B&H17Plu$3428 is the most secure password because it contains:

- Upper case letters,
- Lower case letters,
- Numbers, and
- Special characters.

Email and Internet Security

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Cyber Crime

Cyber crime refers to any crime that involves a computer and a network. Offenses are primarily committed through the Internet.

- Common examples of cyber crime include:
  - Credit card fraud;
  - Spam; and
  - Identity theft.
- Government information and information system assets are a high value target.
- Criminals, terrorists, and nation states with malicious intent work daily to steal, disrupt, and change information systems at government agencies, including HHS.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Social Engineering

These individuals may look trust worthy, but in fact are sophisticated cyber criminals.

They use social engineering techniques to obtain your personal information, access sensitive government information, and even steal your identity.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Social Engineering

- **Social engineering** is classically defined as the art of manipulating and exploiting human behavior to gain unauthorized access to systems and information for fraudulent or criminal purposes.
- Social engineering attacks are more common and more successful than computer hacking attacks against the network.

Objective

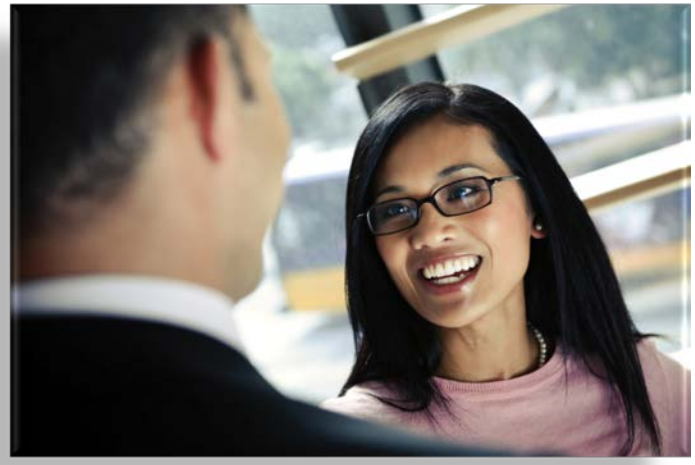
✓ Recognize threats to information systems and privacy

Email and Internet Security

Human Behavior

Social engineering attacks are based on natural human desires like:

- Trust
- Desire to help
- Desire to avoid conflict
- Fear
- Curiosity
- Ignorance and carelessness



Social engineers will gain information by exploiting the desire of humans to trust and help each other.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Targets

Social engineers want any information that will give them access to government systems or facilities. Common targets are:

- Passwords
- Security badges
- Access to secure areas of the building
- Uniforms
- Smart phones
- Wallets
- Employee's personal information

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Phishing Attacks

- Phishing is a social engineering scam whereby intruders seek access to your personal information or passwords by posing as a legitimate business or organization with legitimate reason to request information.
- Usually an email (or text) alerts you to a problem with your account and asks you to click on a link and provide information to correct the situation.
- These emails look real and often contain the organization's logo and trademark. The URL in the email resembles the legitimate web address. For example "Amazons.com".

Spear phishing is an attack that targets a specific individual or business. The email is addressed to you and appears to be sent from an organization you know and trust, like a government agency or a professional association.

Whaling is a phishing or spear phishing attack aimed at a senior official in the organization.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Phishing Examples

Phishing emails appear to be legitimate. Take a look at these real-life examples.

Better Business Bureau complaint. Executives receive an email that looks like it comes from the Better Business Bureau. The message either details a complaint a customer has supposedly filed or claims the company has been accused of identity theft. The recipient is asked to click a link to contest the claim. Once the link is clicked, a computer virus is downloaded.

Travel trouble. An email appears to be a notice from an airline that you have purchased a ticket and arranged to check several bags. Many consumers, outraged because they never planned any such trip, click a link in the email to complain. The problem is, this clicking leads to an identity-theft page, where victims are asked to share sensitive data. If you receive such an email, simply ignore it.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Combat Phishing

- **NEVER** provide your password to anyone via email.
- Be suspicious of any email that:
  - Requests personal information.
  - Contains spelling and grammatical errors.
  - Asks you to click on a link.
  - Is unexpected or from a company or organization with whom you do not have a relationship.
- If you are suspicious of an email:
  - **Do not** click on the links provided in the email.
  - **Do not** open any attachments in the email.
  - **Do not** provide personal information or financial data.
  - **Do** forward the email to the HHS Computer Security Incident Response Center (CSIRC) at csirc@hhs.gov and then delete it from your Inbox.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Identity Theft

- The Federal Trade Commission estimates that 9 million people have their identity stolen each year.
- Identity thieves use names, addresses, Social Security numbers, and financial information of their victims to obtain credit cards, loans, and bank accounts for themselves.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Identity Theft

If you believe you are a victim of identity theft

- Contact the three credit reporting companies (Equifax, Experian, and Trans Union) and place a fraud alert on your report.
- Inform your bank, credit card issuers and other financial institutions that you are a victim of identity theft.
- If you know who stole your information, contact the police and file a report.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Preventing Identity Theft

Combat identity theft

- Be cautious when providing your Social Security number. Know how and why it will be used.
- Review credit card and bank statements at least monthly for unauthorized transactions.
- Use strong passwords for your home computer and web sites you visit, especially email accounts and financial institutions.
- Leave your Social Security card and passport at home. Never leave them in your purse or wallet unless necessary.
- Shred sensitive documents and mail containing your name and address.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Malware

Malware (short for malicious software) does damage to, steals information from, or disrupts a computer system.

- Malware is commonly installed through email attachments, downloading infected files, or visiting an infected web site.
- It can corrupt files, erase your hard drive, or give a hacker access to your computer.

Combat malware

- Read email in plain text and do not use the preview pane.
- Scan attachments with antivirus software before downloading. Do not trust any attachments, even those that come from recognized senders.
- Delete suspicious emails without opening them.
- If you believe your computer is infected, send an e-mail to spam@hhs.gov or contact the security POC.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Internet Hoaxes

Email messages that promise a free gift certificate to your favorite restaurant, plead for financial help for a sick child, or warn of a new computer virus are typically hoaxes designed for you to forward them to everyone you know.

- Mass distribution of email messages floods computer networks with traffic slowing them down. This is a type of distributed denial-of-service (DDoS) attack.

Combat Internet Hoaxes

- Do not forward chain letters, email spam, inappropriate messages, or unapproved newsletters and broadcast messages. This is a violation of the *HHS-OCIO Policy for Personal Use of Information Technology Resources*.
- Do not open emails from senders whom you do not recognize or if you are suspicious that the email could be a hoax.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Spam

Email spam is unsolicited messages sent to numerous recipients, similar to junk mail.

- Spam is dangerous because it can contain links that direct you to phishing websites or install malware on your computer.
- Studies estimate that between 70% and 95% of emails sent are spam.

Combat spam

- **NEVER** click on links or download attachments from spam email
- Only provide your email address for legitimate business purposes.
- Do not sign web site guest books and limit mailing list subscriptions. Spammers access these to obtain your email address.
- Spam received in your government email account should be forwarded to spam@hhs.gov or the security POC.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Appropriate Use of Email

- HHS email accounts are for official business.
- Employees are permitted limited personal use of email.
- Personal emails should not:
  - Disrupt employee productivity;
  - Disrupt service or cause congestion on the network. For example sending spam or large media files; and/or
  - Engage in inappropriate activities.

- Review the *Rules of Behavior for Use of HHS Information Resources* for more information.
- Emails that contain sensitive data must be encrypted before being sent. Information on encryption solutions can be found at: http://intranet.hhs.gov/it/cybersecurity/enterprise_security/Encryption/index.html

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Peer to Peer Software

- Peer to peer, or P2P, is typically used to download copyrighted files like music. Downloading files in this manner is illegal, unethical and prohibited on government-owned computers and networks.

- Some P2P software may be necessary to meet a business need, in which case you may use it, but only with permission from the OpDiv CIO. Speak to your manager for more information.

Objective

✓ Recognize threats to information systems and privacy

Email and Internet Security

Cookies

A cookie is a text file that a website puts on your hard drive that saves information that you typed in like preferences or user name.

- Cookies can also be used to track your activities on the web.
- Cookies pose a security risk because someone could access your personal information or invade your privacy.

Combat cookies

- Use cookies with caution.
- Confirm that web sites that ask for personal information are encrypted and the URL begins with “https”.
- Note that there is an inherent risk anytime you enter personal information on a web site.

Objective

✓ Recognize threats to information systems and privacy

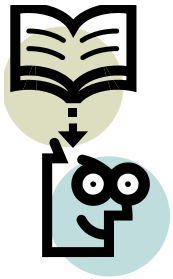
Email and Internet Security

ActiveX

- ActiveX is a form of mobile code technology that allows Internet browsers to run small applications online.
- They pose a security risk because the code alters your computer's operating system. This is a problem if the code is malicious.

Protect your computer

- Require confirmation before enabling ActiveX or other types of mobile code technology.



Knowledge Check

A phishing email:

- A: Is a type of social engineering attack.
- B: Can be from an organization that you recognize, like a professional association.
- C: Contains a link to a web site that asks you for personal information.
- D: All of the above.

Email and Internet Security

Knowledge Check - Answer

The correct answer is:

- Phishing emails are social engineering attacks.
- The emails seem like they are sent from an organization that you know and trust, like a financial institution or professional association.
- Phishing emails always ask for personal information.

Security Outside of the Office

Objective

✓ Identify best practices to secure IT assets and data in and out of the office.

Security Outside of the Office

Did You Know?

Security researchers say that 35% of data breaches at U.S. companies are caused by employees losing laptops or other mobile devices.

Source: SecuritySense Newsletter, April 2012.

Objective

✓ Identify best practices to secure IT assets and data in and out of the office.

Security Outside of the Office

Travel

- Technology, telework, and job duties mean that many employees regularly work away from the office.

Be vigilant about protecting information and information systems outside of the office.

Objective

✓ Identify best practices to secure IT assets and data in and out of the office.

Security Outside of the Office

Protect Information Systems While on Travel

- ✓ Always maintain possession of your laptop and other mobile devices.
- ✓ Ensure that the wireless security features are properly configured.
- ✓ Be cautious when establishing a VPN connection through a non-secure environment (e.g., hotel). Do not work on sensitive material when using an insecure connection.
- ✓ Turn off/disable wireless capability when connected via LAN cable.
- ✓ Turn off your laptop while travelling so that encryption is enabled.
- ✓ Report a loss or theft of your laptop or other government furnished device immediately to your security POC.

Objective

✓ Identify best practices to secure IT assets and data in and out of the office.

Security Outside of the Office

Telework

- You must receive approval and satisfy HHS requirements for telework. For more information see the:
  - *Rules of Behavior for Use of HHS Information Technology Resources;*
  - *HHS-OCIO Policy for Personal Use of Information Technology Resources; and*
  - *HHS Policy for Information Technology Security for Remote Access.*

Protect information and data while teleworking

- Always keep your laptop in sight to prevent loss or theft.
- Only use authorized equipment in authorized locations.
- Use a screen protector so sensitive information cannot be seen by others.
- Report lost or stolen equipment immediately.

Objective

✓ Identify best practices to secure IT assets and data in and out of the office.

Security Outside of the Office

Home Security

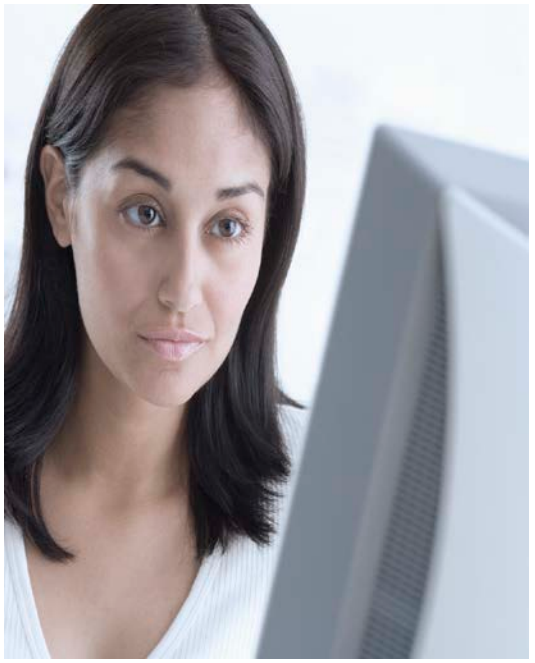
Many of the tips in this course can be used to protect your home computer.

- Criminals can use your personal information to steal your identity and ruin your finances.
- Protecting yourself and your family on the Internet at home is just as important as protecting information systems at work.

Follow these important steps to safeguard your home computer

- Use passwords on personal computers and mobile devices.
- Install and update antivirus software on your home computer.
- Enable the firewall on your computer.
- Routinely backup your files.
- Follow the instructions in the user manual to enable encryption for your wireless router.

Privacy



Objective

✓ Define privacy and PII

Privacy

What is Privacy?

Privacy is a set of fair information practices to ensure:

- Personal information is accurate, relevant, and current.
- All uses of information are known and appropriate.
- Personal information is protected.

Privacy also:

- Allows individuals a choice in how their information is used or disclosed.
- Assures that personal data will be used and viewed for business purposes only.
- Enables trust between HHS and the American public.

Objective
✓ Define privacy and PII

Privacy
Protect Privacy

Protecting personal information is essential at HHS.

Successfully achieving HHS' mission depends on protecting personally identifiable information from loss, theft, or misuse.

Objective
✓ Define privacy and PII

Privacy

Personally Identifiable Information

- Personally identifiable information (PII) can be used to distinguish or trace someone's identity, or can be linked to a specific individual.
- Any such item of information can be PII, including:
  - Sensitive data - medical, financial, or legal information;
  - "Neutral" information - name, facial photos, work address; or
  - Contextual information - file folder for a specific health condition that contains a list of treated patients.

- The type of information determines the protections required by law. For example:
  - HIPAA for some types of health information.
  - The Paperwork Reduction Act for information collected from citizens.
- PII must be protected, whether in paper, electronic, or oral form.

Objective
✓ Define privacy and PII

Privacy

Common Examples of PII

- Name
- Social Security number (SSN)
- Date of birth (DOB)
- Mother's maiden name
- Financial records
- Email address
- Driver's license number
- Passport number
- Personal Health Information (PHI)

Objective
✓ Define privacy and PII

Privacy

PII in Context

What is the chance that you can successfully identify a person with only this information?

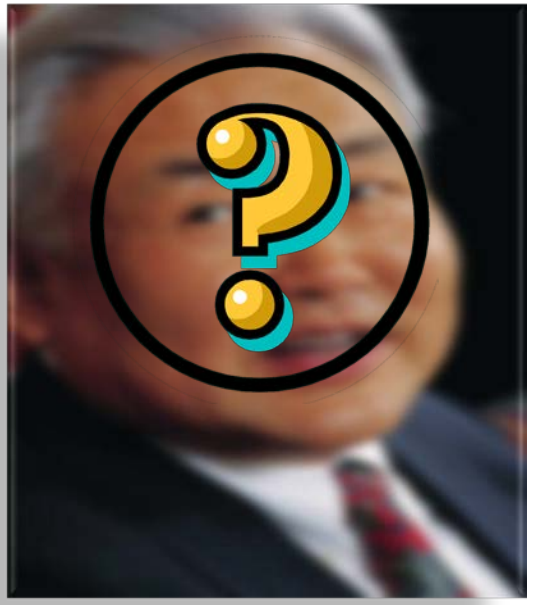
Mr. X lives in ZIP code 02138 and was born July 31, 1945.

A) 1%

B) 87%

C) 50%

D) 34%



(Source: "What Information is 'Personally Identifiable?", Electronic Frontier Foundation by September 11, 2009.)

The answer is **B**. Latanya Sweeney, a Carnegie Mellon University computer science professor, demonstrated that a person's gender, zip code, and date of birth could be used to identify an individual 87% of the time.

Objective

✓ Define privacy and PII

Privacy

PII in Context

Seemingly innocuous information can identify an individual when combined with other data or compared to a data set that includes other PII. Professor Sweeney compared the list of gender, zip codes, and dates of birth with voter registration records for her research.

PII must be protected at all times even if the information cannot be used singularly to identify individuals.

Objective

✓ Recognize threats to information systems and privacy

Privacy

Spillage

Spillage is the improper storage, transmission or processing of PII.

Combat spillage

- Share information on a need to know basis.
- Never access PII unless authorized to do so to perform your job.
- Only store PII on encrypted devices.
- Encrypt emails and double-check that the recipient name(s) is correct before sending.
- When faxing, confirm that you have the correct fax number and call the recipient to confirm receipt.

Objective

✓ Understand personal responsibility to protect information systems

Privacy

Roles and Responsibilities

As a member of the HHS workforce, you are responsible for following privacy policies and procedures.

Privacy policies and procedures require you to:

- Collect, use, and disclose personal information only for reasons that are for a legitimate job function, support the mission of HHS, and are allowed by law.
- Access information only for authorized purposes.
- Safeguard personal information in your possession, whether it be in paper or electronic format.
- Report suspected privacy violations or incidents.
- Shred documents containing PII; **NEVER** place them in the trash. Contact the IT Department for proper disposal of equipment like copy machines and computers.

Objective

✓ Understand personal responsibility to protect information systems

Privacy

Consequences of Privacy Violations

Privacy violations can result in severe consequences including:

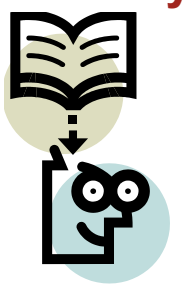
Employee discipline

Fines

Imprisonment

Refer to the Rules of Behavior for Use of HHS Information Resources for more information.

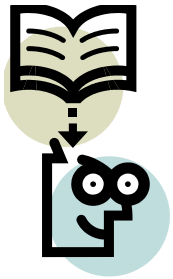
Privacy



Knowledge Check

True or False. Only PII that can be used to directly identify an individual needs protection.

Privacy



Knowledge Check - Answer

The correct answer is:

False

Seemingly harmless PII, like gender or a spouse's name, can still be used to identify a person and must be protected.

Incident Reporting

Objective

✓ Identify the correct way to respond to a suspected or confirmed security or privacy incident

Incident Reporting

Privacy & Data Incidents

- Privacy and data incidents can result in:
  - Inability for HHS to fulfill its mission;
  - Disruption of day-to-day operations;
  - Damage to the reputation of HHS; and
  - Harm to an individual's health or financial status.
- In the case of data being lost, stolen or misused, it is important to respond appropriately.

A prompt and correct response could limit the severity of the incident and protect privacy of individuals.

Objective

✓ Identify the correct way to respond to a suspected or confirmed security or privacy incident

Incident Reporting

Common Scenarios

Privacy incidents most often occur from:

- Loss, damage, theft, or improper disposal of equipment, media, or papers containing PII.
- Accidentally sending a report containing PII to a person not authorized to view the report or sending it in an unprotected manner (e.g., unencrypted).

- Allowing an unauthorized person to use your computer or credentials to access PII.
- Discussing work related information, such as a person's medical records, in a public area.
- Accessing the private records of friends, neighbors, celebrities, etc. for casual viewing.
- Any security situation that could compromise PII (e.g., virus, phishing email, social engineering attack).

Objective

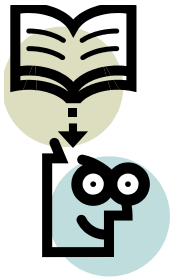
✓ Identify the correct way to respond to a suspected or confirmed security or privacy incident

Incident Reporting

Report an Incident

- Do not investigate the incident on your own - *immediately* report suspected incidents, especially those that could compromise PII, regardless of whether it is in electronic, paper, or oral format.
- Any employee can report an incident. You are not required to speak to your manager before reporting an incident but should keep management informed when incidents occur.
- Report incidents to your OpDiv Computer Security Incident Response Team (CSIRT)/Incident Response Team (IRT). Contact information for each OpDiv can be found at: http://intranet.hhs.gov/it/cybersecurity/hhs_csirc/
- You can also report directly to the HHS CSIRC by email csirc@hhs.gov or phone 866-646-7514.

Incident Reporting



Knowledge Check

Amy left her laptop in a taxi cab on the way to the airport. What should she do? *(choose the best answer)*

- A: Nothing. The files were backed up anyway.
- B: Cancel the trip.
- C: Report the laptop missing to the OpDiv CSIRT.
- D: Buy a new laptop as a replacement.

Incident Reporting

Knowledge Check - Answer

The correct answer is:

Contact the OpDiv CSIRT as soon as you notice a laptop or other mobile device missing or stolen.

Summary

Summary

Objectives

You should now be able to:

- ✓ Define information systems security;
- ✓ Identify federal regulations that mandate the protection of IT assets;
- ✓ Understand HHS' IT security policy, procedures, and practices;
- ✓ Understand personal responsibility to protect information systems;
- ✓ Recognize threats to information systems and privacy;
- ✓ Identify best practices to secure IT assets and data in and out of the office;
- ✓ Define privacy and personally identifiable information (PII); and
- ✓ Identify the correct way to respond to a suspected or confirmed security or privacy incident.

Congratulations

You have completed the Information Systems Security Awareness!

Click Next to read and acknowledge the *HHS Rules of Behavior (For Use of HHS Information Technology Resources).*

HHS Rules of Behavior

Rules of Behavior for Use of HHS Information Resources
Office of the Chief Information Officer
Office of the Assistant Secretary for Administration
Department of Health and Human Services

July 24, 2013

Project: HHS-OCIO Standard RoB
Document Number: HHS-OCIO-2013-0003S

This Department of Health and Human Services (HHS or Department) standard is effective immediately:

The *Rules of Behavior for Use of HHS Information Resources* (HHS RoB) provides the rules that govern the appropriate use of all HHS information resources for Department users, including federal employees, contractors, and other system users. The HHS RoB, in conjunction with the *HHS Policy for Personal Use of Information Technology Resources* [1](as amended), are issued under the authority of the *Policy for Information Systems Security and Privacy (IS2P).*[2] The prior HHS RoB (dated August 26, 2010) is made obsolete by the publication of this updated version.

All new users of HHS information resources must read the HHS RoB and sign the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks. This acknowledgement must be completed annually thereafter, which may be done as part of annual HHS Information Systems Security Awareness Training. By signing the form users reaffirm their knowledge of, and agreement to adhere to, the HHS RoB. The HHS RoB may be presented to the user in hardcopy or electronically. The user's acknowledgement may be obtained by written signature or, if allowed per Operating Division (OpDiv) or Staff Division (StaffDiv) policy and/or procedure, by electronic acknowledgement or signature.

[1] Available at: http://www.hhs.gov/ocio/policy/index.html
[2] Available at: http://www.hhs.gov/ocio/policy/index.html

HHS Rules of Behavior

The HHS RoB cannot account for every possible situation. Therefore, where the HHS RoB does not provide explicit guidance, personnel must use their best judgment to apply the principles set forth in the standards for ethical conduct to guide their actions.

Non-compliance with the HHS RoB may be cause for disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include one or more of the following actions:[3]

- Suspension of access privileges;
- Revocation of access to federal information, information systems, and/or facilities;
- Reprimand;
- Termination of employment;
- Removal or disbarment from work on federal contracts or projects;
- Monetary fines; and/or
- Criminal charges that may result in imprisonment.

HHS OpDivs may require users to acknowledge and comply with OpDiv-level policies and requirements, which may be more restrictive than the rules prescribed herein. Supplemental rules of behavior may be created for specific systems that require users to comply with rules beyond those contained in this document. In such cases users must also sign these supplemental rules of behavior prior to receiving access to these systems[4] and must comply with ongoing requirements of each individual system to retain access (such as re-acknowledging the system-specific rules by signature each year). System owners must document any additional system-specific rules of behavior and any recurring requirement to sign the respective acknowledgement in the security plan for their systems. Each OpDiv Chief Information Officer (CIO) must implement a process to obtain and retain the signed rules of behavior for such systems and must ensure that user access to such system information is prohibited without a signed

[3] Refer to the Employee Standards of Conduct published by the U.S. Office of Government Ethics, available at: http://www.oge.gov/Laws-and-Regulations/Employee-Standards-of-Conduct/Employee-Standards-of-Conduct

[4] National Institute of Standards and Technology (NIST) Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, defines an "information system" as: "A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

HHS Rules of Behavior

acknowledgement of system-specific rules and a signed acknowledgement of the HHS RoB.

National security systems, as defined by the Federal Information Security Management Act (FISMA), must independently or collectively implement their own system-specific rules.

These HHS RoB apply to local, network, and remote use[5] of HHS information (in both electronic and physical forms) and information systems by any individual.
Users of HHS information and systems must acknowledge the following statements:

I assert my understanding that:

- Use of HHS information and systems must comply with Department and OpDiv policies, standards, and applicable laws;
- Use for other than official assigned duties is subject to the *HHS Policy for Personal Use of IT Resources*, (as amended);[6]
- Unauthorized access to information or information systems is prohibited; and
- Users must prevent unauthorized disclosure or modification of sensitive information.[7]

[5] Refer to the glossary of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* for definitions of local, network, and remote access.
[6] Available at: *http://www.hhs.gov/ocio/policy/index.html*.
[7] HHS Memorandum: *Updated Departmental Standard for the Definition of Sensitive Information* (as amended) is available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html.

HHS Rules of Behavior

I must:

General Security Practices

- Follow HHS security practices whether working at my primary workplace or remotely;
- Accept that I will be held accountable for my actions while accessing and using HHS information and information systems;
- Ensure that I have appropriate authorization to install and use software, including downloaded software on HHS systems and that before doing so I will ensure that all such software is properly licensed, approved, and free of malicious code;
- Wear an identification badge (or badges, if applicable) at all times, except when they are being used for system access in federal facilities;
- Lock workstations and remove Personal Identity Verification (PIV) cards from systems when leaving them unattended;
- Use assigned unique identification and authentication mechanisms, including PIV cards, to access HHS systems and facilities;
- Complete security awareness training (i.e., HHS Information Systems Security Awareness Training) before accessing any HHS system and on an annual basis thereafter and complete any specialized role-based security or privacy training, as required by HHS policies;[8]
- Permit only authorized HHS users to use HHS equipment and/or software;
- Take all necessary precautions to protect HHS information assets[9] (including but not limited to hardware, software, personally identifiable information (PII), protected health information (PHI), and federal records [media neutral]) from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and treat such assets in accordance with any information handling policies;

[8] HHS Memorandum: *Role-Based Training (RBT) of Personnel with Significant Security Responsibilities* (available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html) defines the types of positions requiring specialized training.

[9] HHS IT assets are defined as hardware, software, systems, services, and related technology assets used to execute work on behalf of HHS. Definition is adapted from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments.

HHS Rules of Behavior

- Immediately report to the appropriate incident response organization or help desk (pursuant to OpDiv policy and/or procedures) all lost or stolen HHS equipment; known or suspected security incidents;[10] known or suspected information security policy violations or compromises; or suspicious activity in accordance with OpDiv procedures;
- Notify my OpDiv/StaffDiv Personnel Security Representative (PSR) when I plan to bring government-owned equipment on foreign travel (per requirements defined by the Office of Security and Strategic Information (OSSI));[11]
- Maintain awareness of risks involved with clicking on e-mail or text message web links; and
- Only use approved methods for accessing HHS information and HHS information systems.

Privacy

- Understand and consent to having no expectation of privacy while accessing HHS computers, networks, or e-mail;
- Collect information from members of the public only as required by my assigned duties and permitted by the Privacy Act of 1974, the Paperwork Reduction Act, and other relevant laws;
- Release information to members of the public including individuals or the media only as allowed by the scope of my duties and the law;
- Refrain from accessing information about individuals unless specifically authorized and required as part of my assigned duties;
- Use PII and PHI only for the purposes for which it was collected and consistent with conditions set forth by stated privacy notices such as those provided to individuals at the point of data collection and published System of Records Notices; and
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary and to the extent possible, to assure fairness in making determinations about an individual.

[10] Known or suspected security incidents involve the actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information maintained by or in the possession of HHS or information processed by contractors and third-parties on behalf of HHS.
[11] OSSI policies for foreign travel can be found at: http://intranet.hhs.gov/security/ossi/foreign/index.html

HHS Rules of Behavior

Sensitive Information

- Treat computer, network and web application account credentials as private sensitive information and refrain from sharing accounts;
- Secure sensitive information, regardless of media or format, when left unattended;
- Keep sensitive information out of sight when visitors are present;
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with the *HHS Policy for Records Management*[12] and sanitization policies, or as otherwise lawfully directed by management;
- Access sensitive information only when necessary to perform job functions; and
- Properly protect (e.g., encrypt) HHS sensitive information at all times while stored or in transmission, in accordance with the *HHS Standard for Encryption of Computing Devices*.[13]

I must **not**:

- Violate, direct, or encourage others to violate HHS policies or procedures;
- Circumvent security safeguards, including violating security policies or procedures or reconfiguring systems, except as authorized;
- Use another person's account, identity, password/passcode/PIN, or PIV card or share my password/passcode/PIN;
- Remove data or equipment from the agency premises without proper authorization;
- Use HHS information, systems, and hardware to send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums;
- Exceed authorized access to sensitive information;
- Share or disclose sensitive information except as authorized and with formal agreements that ensure third-parties will adequately protect it;

[12] Available at: http://www.hhs.gov/ocio/policy/index.html
[13] Available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html

HHS Rules of Behavior

- Transport, transmit, e-mail, remotely access, or download sensitive information unless such action is explicitly permitted by the manager or owner of such information and appropriate safeguards are in place per HHS policies concerning sensitive information;
- Use sensitive information for anything other than the purpose for which it has been authorized;
- Access information for unauthorized purposes;
- Use sensitive HHS data for private gain or to misrepresent myself or HHS or for any other unauthorized purpose;
- Store sensitive information in public folders or other insecure physical or electronic storage locations;
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information;
- Copy or distribute intellectual property including music, software, documentation, and other copyrighted materials without written permission or license from the copyright owner;
- Modify or install software without prior proper approval per OpDiv procedures;
- Conduct official government business or transmit/store sensitive HHS information using non-authorized equipment or services; or
- Use systems (either government issued or non-government) without the following protections in place to access sensitive HHS information:
    - Antivirus software with the latest updates;
    - Anti-spyware and personal firewalls;
    - A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access; and
    - Approved encryption[14] to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e-mail or remote connections.

[14] Refer to the HHS Standard for Encryption of Computing Devices, available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html.

HHS Rules of Behavior

I must refrain from the following activities when using federal government systems, which are prohibited per the *HHS Policy for Personal Use of Information Technology Resources,*[15] (as amended):

- Unethical or illegal conduct;
- Sending or posting obscene or offensive material;
- Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages;
- Sending messages supporting prohibited partisan political activity as restricted under the Hatch Act;[16]
- Conducting any commercial or for-profit activity;
- Using peer-to-peer (P2P) software except for secure tools approved in writing by the OpDiv CIO (or designee) to meet business or operational needs;
- Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive text or images, or other offensive material;
- Creating and/or operating unapproved Web sites or services;
- Allowing personal use of HHS resources to adversely affect HHS systems, services, and co-workers (such as using non-trivial amounts of storage space or bandwidth for personal digital photos, music, or video);
- Using the Internet or HHS workstation to play games or gamble; and
- Posting Department information to external newsgroups, social media and/other types of third-party website applications,[17] or other public forums without authority, including information which is at odds with departmental missions or positions. This includes any use that could create the perception that the communication was made in my official capacity as a federal government employee, unless I have previously obtained appropriate Department approval.

[15] Available at: http://www.hhs.gov/ocio/policy/index.html.
[16] For additional guidance refer to http://www.osc.gov/hatchact.htm and 5 C.F.R. Part 2635: Standards of ethical conduct for employees of the executive branch.
[17] Refer to the HHS Policy for Managing the Use of Third-Party Websites and Applications, available at http://www.hhs.gov/ocio/policy/index.html.

HHS Rules of Behavior Acknowledgement

ACKNOWLEDGEMENT PAGE

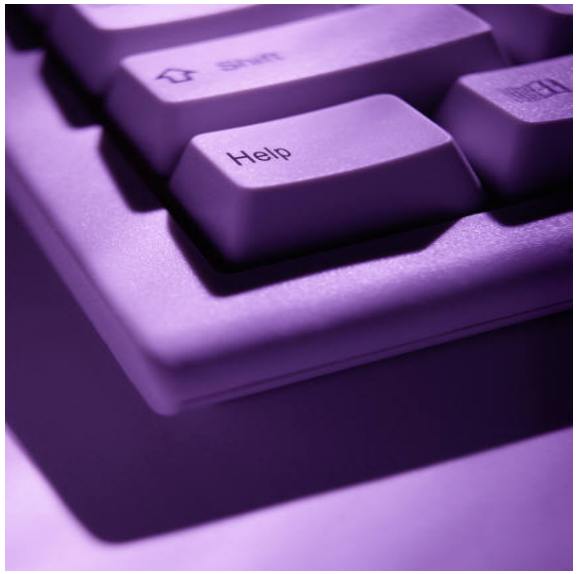
By completing this course, I acknowledge that I have read the *HHS Rules of Behavior* (HHS RoB), version HHS-OCIO-2013-0003S, dated July 24, 2013 (or as amended) and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities; and may also include criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

APPROVED BY AND EFFECTIVE ON:

/s/ July 24, 2013

Frank Baitman DATE
HHS Chief Information Officer

Appendix


Help


court to
on, a matter
SYN.
ref·er·ence
referred, esp.,
person, committee,
connection; regard
4. a)

Appendix

HHS Resources

- The **HHS Cybersecurity Program** is the Department‘s enterprise-wide information security and privacy program, helping to protect HHS against potential IT threats and vulnerabilities. The Program plays an important role in protecting HHS' ability to provide mission-critical operations, and is an enabler for e-government.
- HHS Cybersecurity Program Support provides assistance with IT security and privacy related issues. HHS Cybersecurity Program Support is staffed Monday through Friday from 9:00 AM to 5:00 PM eastern standard time (EST).

Web: http://intranet.hhs.gov/it/cybersecurity/index.html

Phone: (202) 205-9581

E-mail: HHS.Cybersecurity@hhs.gov

Appendix

HHS Resources

- Information pertaining to the HHS Information Security and Privacy Program can be found at: http://www.hhs.gov/ocio/securityprivacy/index.html.

- Information pertaining to Federal cybersecurity and privacy legislation can be found at: http://www.hhs.gov/ocio/securityprivacy/pglandreports/polguidlegrep.html.

- The *HHS-OCIO Policy for Information Systems Security and Privacy* establishes comprehensive IT security and privacy requirements for the IT security programs and information systems of OpDivs and StaffDivs within HHS. It can be found at: http://www.hhs.gov/ocio/policy/index.html#Security.

Appendix

Privacy Points of Contact

For specific privacy-related questions, contact:

- OpDiv Senior Official for Privacy (SOP) (http://intranet.hhs.gov/it/cybersecurity/privacy/index.html).
- Privacy Act Contacts (http://www.hhs.gov/foia/contacts/index.html#privacy).