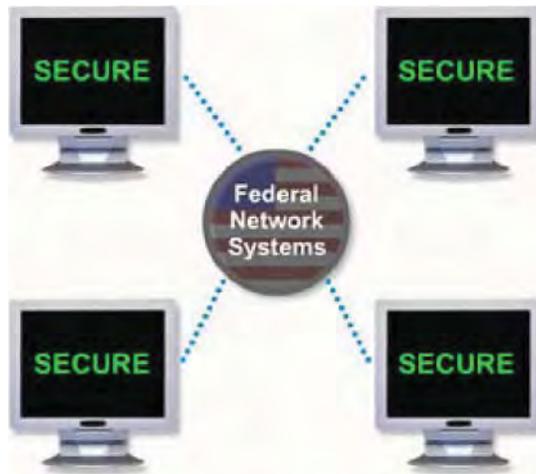




Fiscal Year 2011 Information Security Awareness and Rules of Behavior Training

United States Department of Agriculture



This alternate version of the training is for USDA employees, contractors, partners and volunteers who are unable to complete the training online in AgLearn. However, it is important that users make **every effort to use AgLearn**.

After reading the course material, **you also need to take and pass the assessment** that should have been provided to your supervisor, and acknowledge that you have read the Rules of Behavior. Supervisors are responsible for administering the test and ensuring that the Rules of Behavior have been acknowledged..

A passing score for the assessment is 70%. To obtain **credit for completing** this version of the training, the completion must be reported and recorded. Your agency should provide information on how to accomplish this.

Lesson 1: Course Introduction

Welcome

By taking this course, you are meeting the legal requirement for all users of federal information systems to take annual security awareness training. This course is designed to help you understand the importance of information systems security, or ISS, its guiding principles, and what it means for your agency. This course also provides the "Rules of Behavior" that govern your use of USDA information technology (IT) resources.

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



This course consists of five lessons:

1. The **Course Introduction** will provide you with a brief overview of the course.
2. The **Importance of Information Systems Security** lesson will introduce the principles of ISS, their evolution, and ISS-related policies, laws, and Rules of Behavior. It will also introduce the critical infrastructure protection program.
3. The **Threats to Information Systems Security** lesson will explain the difference between threats and vulnerabilities. It will also provide information regarding various types of threats.
4. The **Malicious Code** lesson will introduce the concept of malicious code, including its impact and the methods used to infect information systems.
5. Finally, the **User Roles and Responsibilities** lesson will identify important guidelines for ensuring a secure system, define classification levels for federal information, and outline your role as a user in protecting this information.

After completing this course, you should be able to:

- Identify what information systems security is and why it is important.
- Explain the difference between a threat and vulnerability, and identify the risks associated with each.
- Understand the threat posed by malicious code and identify how to protect federal information systems from malicious code.
- Explain the classification levels for federal information and identify what you must do to help protect federal information.
- Understand your responsibilities and the "Rules of Behavior" that govern the use of USDA IT resources.

Lesson 2: Importance of Information Systems Security (ISS) and Rules of Behavior



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 our information and information systems.

ISS and Rules of Behavior protect information from unauthorized access or modification and ensure that information systems are available to its users.

This means that a secure information system maintains **confidentiality**, **integrity**, and **availability**.

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 all 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.

ISS and Rules of Behavior Legal Requirements

It is important that you are aware of the possibility of attacks against federal systems and the method in which potential attacks could occur.

Understanding your responsibilities for protecting information resources and how you can contribute to preventing attacks will contribute to the safety of federal information systems.

USDA is required by law to ensure that anyone who utilizes USDA IT resources is aware of his or her responsibilities and complies with the established Rules of Behavior.

The Federal Information Security Management Act, or FISMA (part of the E-Government Act of 2002, Public Law 107-347 dated December 17, 2002), and the Office of Management and Budget, or OMB, Circular A-130 require that all users of federal computer systems be trained in information systems security concerns and comply with the established Rules of Behavior. U.S. Office of Personnel Management, or OPM, regulations also require each agency to have computer security awareness training.



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.

The following nonofficial activities are prohibited on any government owned or leased computer:

- 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 are connected with any type of outside employment.

- Endorsement of any non-government products, services, or organizations.

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:

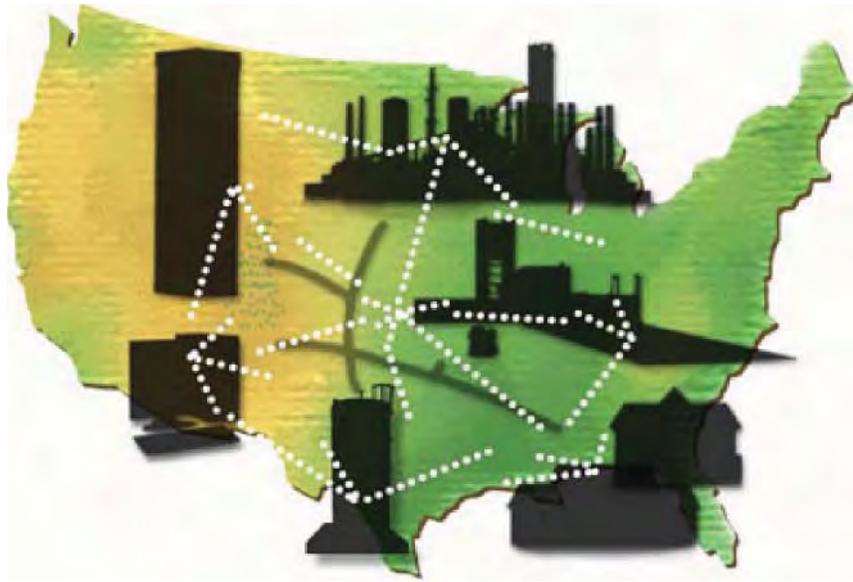
- Corrective actions (taken in accordance with existing rules, regulations, and laws) include:
 - Written reprimands;
 - Temporary suspension from duty;
 - Reassignment or demotion; and
 - Termination of Federal employment.
- Suspension of system privileges.
- Possible criminal prosecution.

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.



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.

Lesson 3: Threats to Information Systems Security

Threats and Vulnerabilities

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 the vulnerability, vendors issue a fix in the form of a patch to the software.

Threat Categories

There are two types of threat categories: environmental and human 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.

Rules of Behavior – Hardware/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;
- Excessive dusty environments; and
- Combustible materials.

Internal vs. External Human Threats

Human threats can be internal or external. An internal threat can be a malicious or disgruntled user, a user in the employ of terrorist groups or foreign countries, or self-inflicted unintentional damage, such as an accident or bad habit.

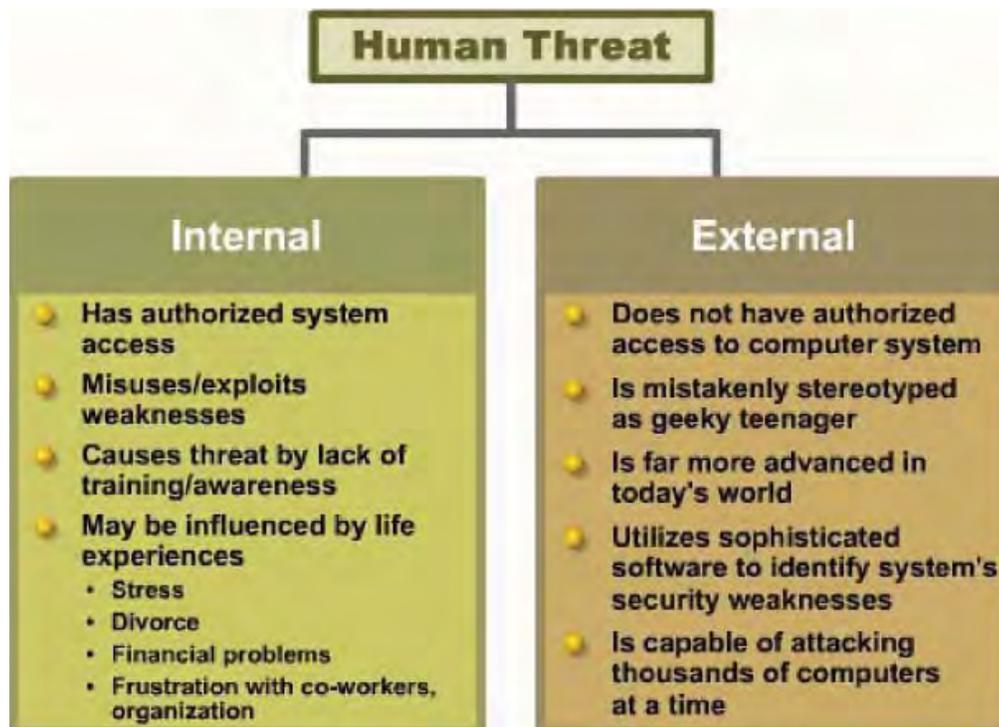
An external threat can be hackers, terrorist groups, foreign countries, or protesters.



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 computer resources.

An internal threat, or insider, is any person with legitimate physical or administrative access to the computer who can misuse or exploit weaknesses in the system. Others, due to a lack of training and awareness, can also cause damage. 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.



Rules of Behavior – Internal Threats

Users shall:

- Keep an inventory of all equipment assigned to them.
- Only use equipment for which they have been granted authorization.
- 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.
- 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.
- 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.

External Threats

External threats, or outsiders, are most commonly hackers. An outsider is an individual who does not have authorized access to an organization's computer system.

Today's hackers may include representatives of foreign countries, terrorist groups, or organized crime. 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 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.



Social Engineering Overview



Social engineering is a hacking technique that relies on human nature. This approach is used by many hackers to obtain information valuable to accessing a secure system.

Rather than using software to identify security weaknesses, hackers attempt to trick an individual into revealing passwords and other information that can compromise your system security.

They use people's inherent nature to trust to learn passwords, logon IDs, server names, operating systems, or other sensitive information.

For example, a hacker may attempt to gain system information from an employee by posing as a service technician or system administrator with an urgent access problem.

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

Your Role in Social Engineering

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.



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

Rules of Behavior – Access/Social Engineering

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

- Protect passwords from access by other individuals.
- Never give a password to another person, including a supervisor or a computer support person.
- Not ask anyone for their password.
- Construct effective passwords by following USDA password policy for complex passwords.

Users shall access and use only information for which they have official authorization. Users shall:

- Follow established procedures for accessing information, including 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 files (i.e., what can be accessed).

Rules of Behavior – Incident Reporting

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

- Report security incidents, or any incidents of suspected fraud, waste, or misuse of USDA resources or USDA personal 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 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 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.

Phishing

A social engineering scam that you need to be aware of is phishing. Phishing is a high-tech scam that uses email or websites to deceive you into disclosing your credit card numbers, bank account information, social security number, passwords, or other sensitive information.

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 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

If you get 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.



A recent real life example of social engineering occurred when a U.S. government employee, visiting another country, provided his business card to several people. A few months later, a highly-visible U.S. government official received an "official-looking" email containing an attachment from a valid ".gov" address. Fortunately, the recipient did not open the email's attachment, but instead, sent the email back to the person whom he thought sent it to him for verification.

It turns out that the originating email spoofed the email address of the government employee who traveled to the foreign country. The attachment contained malicious code.

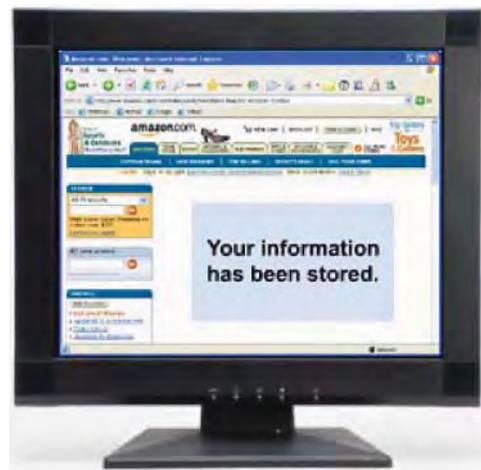


Cookies

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, in order 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 not to accept cookies.

Mobile Code



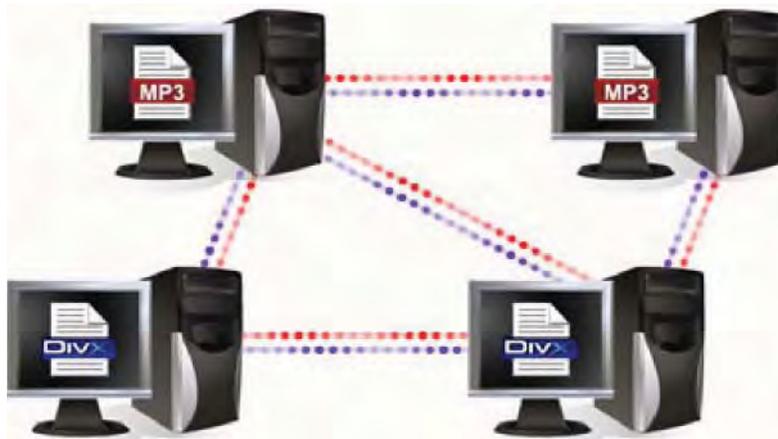
Mobile code, such as ActiveX and Java, are scripting languages used for Internet applications.

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.

Your agency may have developed policy guidance for the use of mobile code. If so, it may restrict the application of mobile code in your agency's information

Peer-to-Peer (P2P)



Peer-to-peer, or P2P, refers to file sharing applications, such as Morpheus and BitTorrent, that enable computers connected to the Internet to transfer files to each other.

Peer-to-peer software enables files to be accessed and transferred with ease.

Music files, pornography, and movie files are the most commonly transferred files using unauthorized peer-to-peer software. Obtaining these files at no cost raises not only ethical concerns, but could result in criminal or civil liability for illegal duplication and sharing of copyrighted material. In addition, participating in peer-to-peer file sharing increases your

vulnerability. Opening up your computer via the Internet provides outsiders a link into your system, creates risk, and enables the possibility for a breach in security.

Peer-to-peer connections are a common avenue for the spread of computer viruses and spyware.



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:

- Yahoo! Messenger
- Windows Live Messenger
- Skype
- AOL Instant Messenger

File Sharing:

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

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.

Rules of Behavior – Peer-to-Peer File Sharing

Users are prohibited from using peer-to-peer (P2P) file sharing. P2P file sharing poses a threat to IT security. It allows employees to transfer files between computers without proper security controls. These programs can be used to distribute inappropriate materials, violate copyright law and put government information at risk. Users should be familiar with the USDA P2P file sharing policy located on the USDA directives Intranet site.

Rules of Behavior – Software

Users shall not install non-authorized, 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 NOT:

- Use USDA purchased software on personally owned or non-USDA computers unless authorized.
- Alter the configuration, including installing software or peripherals, on government computer equipment unless authorized.

In addition, users shall:

- Comply with all software licensing agreements and Federal copyright laws.
- Not 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."

Lesson 4: Malicious Code

What is Malicious Code?

Malicious code is defined as software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.



It is designed with the intent to deny, destroy, modify, or impede system configuration, programs, or data files.

Malicious code comes in several forms including viruses, Trojan horses, and worms.

The most common methods for the spread of malicious code are through email attachments and downloading files from the Internet, but you can also get malicious code just from visiting an infected website.

Email and Attachments



.exe

Email messages and email attachments provide a common route to transfer malicious code.



.com

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. Specific attachments to look for that could contain malicious code are those ending in .exe, .com, .vbs, .bat, and .shs.



.vbs



.bat

Don't assume that an attachment is safe because a friend or coworker sent it. Some malicious code is activated by merely opening the message. Save the attachment to your hard drive and scan it with up-to-date anti-virus software before opening it.



.shs

Protect Your Computer System

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

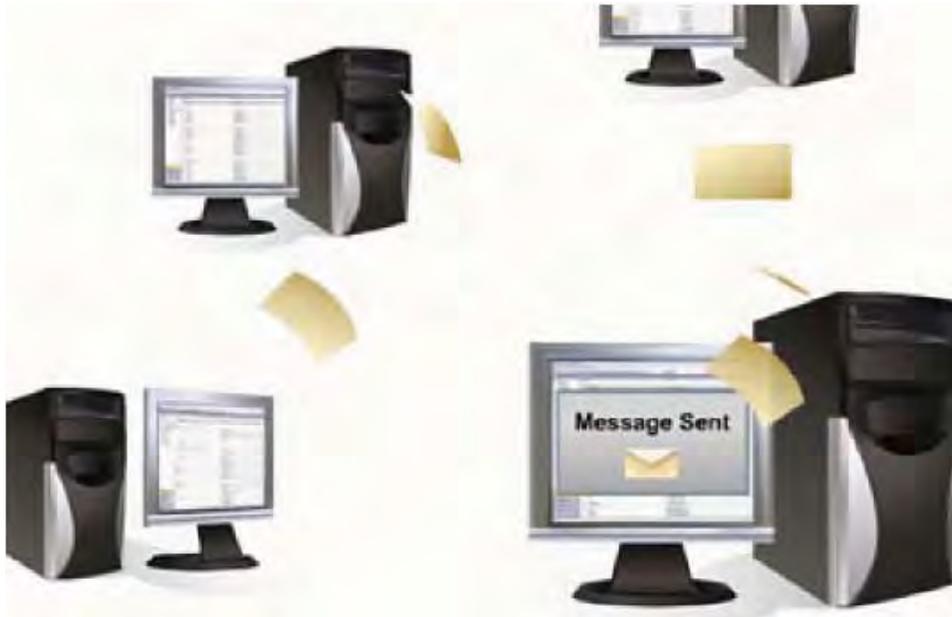
Respond to Virus Attack

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

Hoaxes

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.

Lesson 5: User Roles and Responsibilities

Basic User Guidelines

As an authorized user of federal information systems, you have certain responsibilities when using a government machine.

Remember that your rights to privacy are limited when using government computer resources.

Any activity conducted on a government system can be monitored. Each time you log on to a government system, you consent to being monitored. You should use your computer for government business only.



Avoid government computer misuse. Some examples of computer misuse are: viewing or downloading pornography, gambling on the Internet, conducting private commercial business activities or profit-making ventures, loading personal software, or making unauthorized configuration changes.

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.

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:
 - Using up-to-date anti-virus software.
 - 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 entering unauthorized, inaccurate, or false information into a system.

Appropriate Email Use

Rules of Behavior – Email

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 policy and guidelines.
- Users are prohibited from using USDA IT resources to send, receive, retain, or proliferate any messages or material that is fraudulent, inappropriate, offensive, harassing, or is of a sexual nature.

Usage Guidelines – Email

Email is also for official business. Your organization may 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 to 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.

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.



Tips for Creating a Secure Password

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.

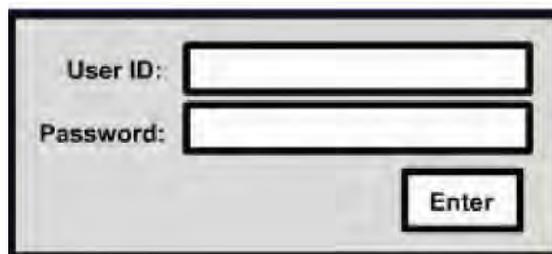
Remember, it is your responsibility to ensure that all activity performed under your user ID is appropriate use of federal information systems resources.

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

- Combine letters, numbers, special characters.
- Use alphanumeric combinations or phrase associations.
- Avoid words or phrases that can be found in the dictionary.
- Avoid using personal information.
- Memorize password and refrain from writing it down.
- Change password regularly.

Physical Security

Protecting federal information systems and the information they contain starts with physical security.



A login form with a light gray background and a black border. It contains two input fields: "User ID:" followed by a white rectangular box, and "Password:" followed by a white rectangular box. Below the password field is a small rectangular button labeled "Enter".

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;
- Locking data storage devices, such as hard drives and USB drives, before you leave for the evening and during emergency procedures such as fire alarms.



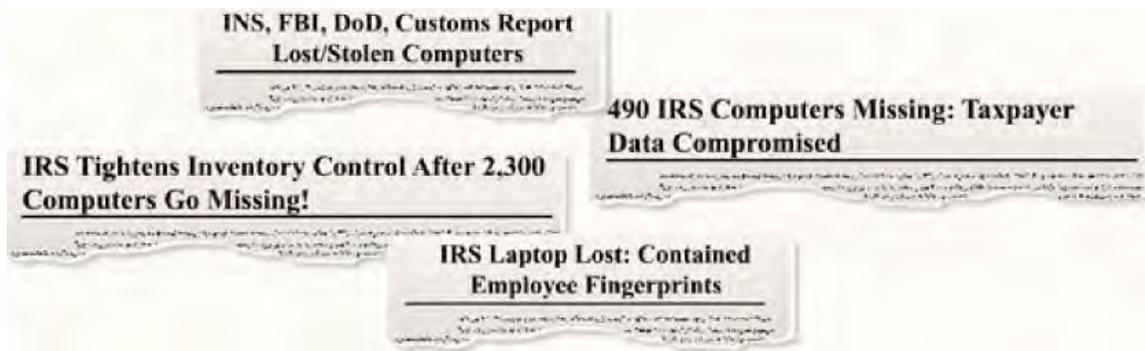
You should also make sure others follow your organization's physical security policies and challenge people who don't. Don't allow people to gain entrance to a building or office by following someone else instead of using their own badge or key code.

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



Teleworking, also known as telecommuting, is emerging as a viable option for many government employees. Advances in computer and telecommunications capabilities make teleworking 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.

Classified and Unclassified Information

All federal information, combined with the right conditions and circumstances, could provide an adversary insight into our capabilities and intentions. In addition, the aggregation of unclassified information can elevate the sensitivity level of information.

Thus, even unclassified information, if compromised, could impact the safety of our personnel and systems.

All federal unclassified information not specifically cleared for public release requires some level of security protection. At a minimum, it must be reviewed before it is released, in any form, outside the U.S. government. Each agency has its own unclassified information policy. Contact your security point of contact for additional information on your agency's policy.

Unclassified Information

- Unclassified information includes “For Official Use Only” or FOUO; “Controlled Unclassified Information” or CUI; and “Sensitive But Unclassified” or SBU.
- Examples are personnel, financial, payroll, medical, operational, and Privacy Act information.
- CUI must be stored in a locked drawer or secure container. When it is no longer needed, it should be destroyed.

Classified information

- Classified information includes “Confidential,” “Secret,” or “Top Secret.”
- The specific level of classification is determined by the original classification authority.
- Classified information must be used in an area that has been approved and cleared for the appropriate classification level.
- When not in use, classified information must be stored in a General Services Administration (GSA) approved vault or container.

Rules of Behavior – Confidential/Sensitive Information

Access to confidential or sensitive information must be restricted to authorized individuals who need it to perform their jobs. This entails refraining from intentional disclosure and using measures to guard against accidental disclosure.

Users shall:

- Protect confidential or sensitive information by using encryption, and limiting the collection, disclosure, sharing and use of PII data. Never access or disclose personal information or other sensitive data unless it is necessary to perform official duties.
- Not send highly sensitive information via email, unless it is encrypted.
- Ensure that sensitive information sent to a fax or printer is handled in a secure manner (e.g., use of a cover sheet that contains a statement that the faxed information is confidential).

In addition, users shall:

- Not store or transmit confidential information on public access systems, such as email or the Internet.
- Lock up media, such as paper copies, tapes, and disks containing confidentially sensitive data. Dispose of media according to approved procedures.
- Never access someone else's account or files without a supervisor's formal authorization.
- To the maximum extent possible, ensure that computer monitors are located in such a way as to eliminate viewing by unauthorized persons.

Users shall also:

- Lock workstations when away from the desk as a preventative measure to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.
- When requesting that another individual receive, pick up or deliver application systems input and output information and media, ensure that the individual is authorized.
- Ensure that confidential or sensitive data are properly erased when disposing of hardware or media.

Backups, Storage, and Labeling

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



It is essential that important files are backed up on a regular basis and stored in a secure location. This will minimize the loss of data if your hard drive crashes or is infected by a virus.

Store all removable media, including CDs, USB drives, and removable hard drives 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 appropriate security classification of information it contains.

When you no longer need the information on the removable media, you should not erase, or "sanitize" the information. Removable media must be degaussed or destroyed if it is not reused at the same or higher classification level of the system in which it was used.



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

Rules of Behavior – Backup, 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. 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.

Media Devices

Be extremely careful when using fax machines, cell phones, laptops, personal digital assistants, or PDAs, and wireless networks. You need to be as vigilant about security on these devices as you are with your computer at work.



Fax Machines

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.

Cell Phones

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.



PDA's



Personal digital assistants, or PDA's, such as BlackBerrys, or Palm Pilots, pose a security threat for a number of reasons.

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

They have tremendous connectivity and storage capabilities, and are extremely popular. It can be very easy for a person to set up a PDA to download information from your computer.

All PDA's connecting to government systems should be in compliance with your agency's policy and OMB guidance.

Laptops



The convenience of laptops and other portable computing devices also makes them extremely vulnerable to theft or security breaches.

User logon information should always be password protected.

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

Maintain possession of your laptop at all times when traveling to prevent theft. When reaching your temporary travel destination, be sure that your laptop is properly secured when left unattended.

If your laptop has wireless capability, ensure that the wireless 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, configured to connect to recognized Internet access points, not ad hoc networks.

The Office of Management and Budget (OMB) issued a memorandum stating that all sensitive data stored on laptops and other portable computer devices should be encrypted. Ensure that you follow both your agency's and OMB's guidance on encryption of sensitive data on laptops.

Wireless Network

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.



Rules of Behavior – Wireless Networks

All USDA employees and contractors are prohibited from using any unauthorized 802.11x network devices within USDA buildings. Users must ensure that any wireless capable devices in their control, including laptops, PDAs, and Bluetooth telephones, have their wireless networking disabled. The only acceptable use of wireless communications is through the USDA provided messaging service.

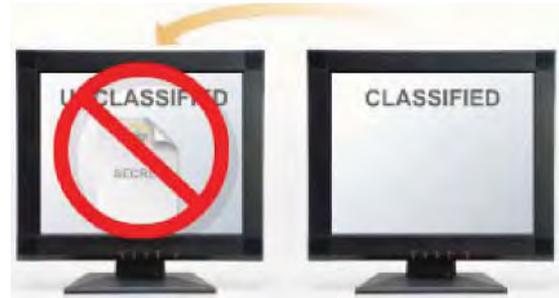
Wireless is vulnerable because unauthorized users may be able to capture not only the data you are transmitting, but also any data stored on your network.

Ensure you are in compliance with your agency's policy regarding the use of wireless technologies.

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.
- Ensure all file names and subject headers reveal the sensitivity of the information.

Personal Identifiable Information



The Privacy Act, signed into law in 1975, requires the government to safeguard information about individuals that is processed by Federal agencies or contractor computer systems. The Act also requires the government to provide access to the information by the individual and to amend the information if it is not accurate, timely, complete, or relevant.

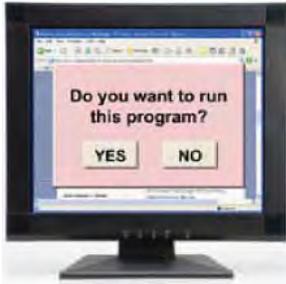
New guidance concerning greater measures for protection of Personal Identifiable Information (PII) is outlined in several OMB memoranda.

For example, OMB requires that lost or stolen PII be reported within one hour to the U.S. Computer Emergency Response Team, or CERT.

Each agency has its own policies to implement OMB's guidance. Check with your security point of contact for additional PII requirements.

As an authorized user, you should ensure that PII is protected on Federal computer systems.

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.

Rules of Behavior - Training

Annual Information Security Awareness and Rules of Behavior Training is mandatory for all USDA employees, contractors, partners, and volunteers. New employees, contractors, partners, and volunteers are required to complete the awareness training prior to gaining access to systems. All users must stay abreast of security policies, requirements, and issues. Users must make a conscientious effort to avert security breaches by staying alert to network vulnerabilities.

USDA Rules Of Behavior – Acknowledgment

There are no exceptions to the requirement that all employees, contractors, partners, and volunteers comply with these rules of behavior. If you are not sure whether your intended computer use is prohibited, you should NOT do it. Consult with your supervisor or appropriate management official for clarification.

USDA requires employees, contractors, partners, and volunteers to acknowledge that they understand their responsibilities and accountability for using USDA information and resources. The completion of this training constitutes the acknowledgment of these USDA Rules of Behavior.

This confirms that I successfully completed the training.

I have read and understand the Rules of Behavior:

Name: _____

Date: _____

Per Departmental Regulation 3620-001, AgLearn is the official training system for USDA, and the source of all data for audits, mandatory training completions, and records examinations relating to personnel actions. All data contained in AgLearn is subject to examination by the USDA Inspector General and/or the Office of Personnel Management without notice at any time. False claims of completed training submitted by employees using AgLearn as recorded in their Learning History file, if substantiated, may be used to support disciplinary or other administrative actions.

**THIS IS THE END OF THE TRAINING MATERIAL.
YOU NOW NEED TO TAKE AND PASS THE ASSESSMENT AND
ACKNOWLEDGE THE RULES OF BEHAVIOR.
PLEASE CONTACT YOUR SUPERVISOR.**

GLOSSARY

Availability

Timely, reliable access to data and information services for authorized users.

Confidentiality

Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Cookie

Text file that a web server stores on your hard drive when you visit a website.

Critical Infrastructure Protection (CIP)

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.

Distributed Denial of Service (DDoS)

DDoS are attacks that are a threat to Internet security. These attacks involve bombarding a web server with huge amounts of data from many different machines and locations in an effort to bring the server down and deny its availability.

Electronic Commerce (e-commerce)

Business transactions conducted using electronic documents, rather than paper.

Information Systems Security (ISS)

Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures used to detect, document, and counter such threats.

Integrity

Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Internet Hoax

Email messages designed to influence you to forward them to everyone you know.

Federal Information Security Management Act (FISMA)

- Mandates a computer security program at all federal agencies.
- Provides for development and maintenance of minimum controls required to protect federal information systems.
- Provides comprehensive framework for ensuring effectiveness of information security controls.
- Requires agencies to identify risk levels and implement appropriate protections.
- Requires each agency to develop and maintain an inventory of major information systems
- Requires government employees and contractors using these systems to undergo periodic computer security training.
- Requires that agencies report to Congress on FISMA compliance.
- Defines national security systems.

Malicious code

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Office of Management and Budget (OMB) Circular A-130, Appendix III

Requires all federal information systems to:

- Possess information security plans;
- Address computer security in reports to Congress through OMB;
- Provide computer security awareness and training for system users, operators, and managers;
- Conduct improved contingency planning;
- Maintain formal emergency response capabilities; and
- Assign a single individual operational responsibility for security.

Peer-to-peer (P2P)

Refers to file sharing applications that enable computers connected to the Internet to transfer files to each other, such as Morpheus and BitTorrent.

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency, including, but not limited to education, financial transactions, medical history, criminal or employment history, and 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, and biometric records, including any other personal information that is linked or linkable to an individual.

Phishing

A high-tech scam that uses email or websites to deceive you into disclosing your credit card numbers, bank account information, social security number, passwords, or other sensitive information.

Spillage

Spillage occurs 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.

Spyware

Malicious software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, without your consent or knowledge.

Threat

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.

Vulnerability

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 the vulnerability, vendors issue a fix in the form of a patch to the software.

THIS IS THE END OF THE TRAINING MATERIAL. YOU NOW NEED TO TAKE AND PASS THE ASSESSMENT AND ACKNOWLEDGE THE RULES OF BEHAVIOR.

Attachment J

Exam Name: USDA-CYBERSECURITY-FY2011

Exam Sequence ID: 24

Date: 9/24/2010

User ID: _____

User Name: _____

1 For Official Use Only (FOUO) and Controlled Unclassified Information (CUI) may include all of the following except:

- A Sensitive information
- B Secret information
- C Payroll information
- D Personnel information

2 All of the following are principles essential to a secure information systems except:

- A Integrity
- B Availability
- C Accountability
- D Confidentiality

3 Both internal and external threats can bring down a system. Which of the following represents an internal threat?

- A Terrorist group
- B Protestors
- C Hackers
- D Disgruntled user

4 A man dressed as a service technician asks Monique for her system passwords so that he can eradicate a problem on her computer. She gives him the passwords. Monique is a victim of:

- A Social engineering
- B Vulnerability
- C Threat
- D Peer-to-peer technology

5 According to the U. S. Department of Justice, what type of fraud is one of the fastest growing white-collar crimes?

- A Internet fraud
- B Online gambling
- C Telephone transfer fraud
- D Pyramid schemes

6 The only acceptable use in this list for any USDA computer asset is:

- A Viewing or downloading pornography.
- B Conducting private commercial business.
- C Gambling on the Internet.
- D Conducting research for a work project.

7 A file with which of the following file extensions is most likely to contain malicious code?

- A .jpg
- B .doc
- C .bat
- D .pdf

8 Edna wants to create a strong password. She should avoid all of the following except:

- A Birthdays
- B Family or pet names
- C Sports teams
- D Special characters

9 All of the following are common ways of spreading malicious code except:

- A Downloading files from the web
- B Peer-to-peer software
- C E-mail attachments
- D Backup important files

10 Which of the following are an example of a security incident?

- A Attempts to send electronic junk mail in the form of commercial announcements.
- B Attempts by unidentified or unauthorized people to obtain sensitive personal or business information.
- C Loss of a government laptop containing personnel information.
- D All of the above

11 What is not PII?

- A Gender
- B Place of birth
- C Employment History
- D Information about or associated with an individual

12 Which of the following will help reduce your risk of identity theft when engaging in e-commerce?

- A Use e-commerce for all transactions.
- B Click on links sent to you from trusted providers.
- C Respond to E-mail inquiries only from institutions you do business with regularly.
- D Confirm the site you are using uses an encrypted link.



USDA Rules Of Behavior – Acknowledgment

There are no exceptions to the requirement that all employees, contractors, partners, and volunteers comply with these rules of behavior. If you are not sure whether your intended computer use is prohibited, you should NOT do it. Consult with your supervisor or appropriate management official for clarification.

USDA requires employees, contractors, partners, and volunteers to acknowledge that they understand their responsibilities and accountability for using USDA information and resources. The completion of this training constitutes the acknowledgment of these USDA Rules of Behavior.

This confirms that I successfully completed the training.

I have read and understand the Rules of Behavior:

Name: _____

Date: _____

Per Departmental Regulation 3620-001, AgLearn is the official training system for USDA, and the source of all data for audits, mandatory training completions, and records examinations relating to personnel actions. All data contained in AgLearn is subject to examination by the USDA Inspector General and/or the Office of Personnel Management without notice at any time. False claims of completed training submitted by employees using AgLearn as recorded in their Learning History file, if substantiated, may be used to support disciplinary or other administrative actions.

**THIS IS THE END OF THE TRAINING MATERIAL.
YOU NOW NEED TO TAKE AND PASS THE ASSESSMENT AND
ACKNOWLEDGE THE RULES OF BEHAVIOR.
PLEASE CONTACT YOUR SUPERVISOR.**

INFORMATION SYSTEM SECURITY
Computer User Security Agreement

As a user of an information system, I _____ will adhere to the following security rules: (Print User Name)

1. I will use USDA computer systems (computers, laptops, PDAs, and networks) only for authorized purposes.
2. If using USDA computer systems and networks for nonofficial purposes, I will do so within the bounds allowed by USDA policy and supervisor approval, and without interfering with official business.
3. I will not use USDA resources, including electronic mail and Internet/Worldwide Web access, for purposes that violate ethical standards, including harassment, threats, sending or accessing sexually explicit material, racially or ethnically demeaning material, gambling, chain letters, for-profit activities, political activities, promotion or solicitation of any activities prohibited by law.
4. I will not load any unapproved software (software from home, games, etc) or install hardware such as peripheral devices (external hard drives, docking stations, etc.) on any USDA system. If I need software or hardware loaded on my system, I will obtain written approval from my supervisor and coordinate the installation with my System Administrator or Help Desk (e.g., Service Center Agencies can only load Common Computing Environment hardware/software certified by the OCIO-ITS IO Lab).
5. I will not download file-sharing software (including MP3 music and video files), peer-to-peer software (i.e. Kazaa, Napster) or games onto my GC, Government IT system, or network.
6. I will not try to access data or use operating systems or programs, except as specifically authorized.
7. I know I will be issued Government user identifiers (user IDs) and passwords to authenticate my computer account. After receiving them—
 - a. If given a password, I will immediately change the password.
 - b. I will not allow anyone else to have or use my password. If I know that my password is compromised, I will report this issue to my supervisor or to my assigned Information System Security Program Manager (ISSPM), or Information System Security Point of Contact (ISSPOC).
 - c. I am responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when I am logged onto a system with that account.
 - d. I will ensure that my password is changed on a regular basis or if it is compromised, whichever is sooner.
 - e. I understand that USDA has a password complexity requirement, and I will use passwords that meet this requirement.
 - f. I will not write down my password or store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), or on any magnetic or electronic media unless approved in writing by the USDA Agency Security Staff.

8. I will log completely off workstations, or use screen savers that require a password to reactivate the workstation; any time I leave the workstation unattended (except in genuine emergencies, such as fire).
9. I will scan all removable media (for example, disks, CDs, thumb drives) for malicious software (for example, viruses, worms, etc) before using it on any government computer, system, or network.
10. I will practice good housekeeping with all electronic equipment, including keeping food, beverages, or other contaminants away from computers and data storage media.
11. I will report promptly to my supervisor and/or to my assigned USDA Agency Security Staff any actual or suspected violation of security.
12. I will stay abreast of security issues via education and awareness products distributed throughout USDA—
 - I have completed the Computer Security Awareness (CSAT) and Privacy Basics Training courses and completion will be recorded in the Agriculture Learning (AgLearn) system.
 - I verify that I have read and will abide by the “Security Expectations and Rules of Behavior” brochure available at: <ftp://ftp-fc.sc.egov.usda.gov/ITC/SecurityBrochures>
 - I verify that I have read the “Security Incident Response Guide for Users” available at: <ftp://ftp-fc.sc.egov.usda.gov/ITC/SecurityBrochures>
 - I verify that I will read and abide by all NRCS Title 270 (Information Resources Management) Electronic Directives System (eDirectives) located via my.NRCS at: <https://my.nrcs.usda.gov/management.aspx> or at <http://directives.sc.egov.usda.gov/>
 - I verify that I will reference (when appropriate) the OCIO-Information Technology Services (ITS) Security Policies located at: http://www.ocionet.usda.gov/ocio/its/security/library/security_Library.asp

I know that my actions as a user can greatly affect the security of the system. My signature on this agreement indicates that I understand my responsibilities as a user of government computer systems and that I adhere to regulatory guidance. I am subject to administrative and/or disciplinary action if I violate USDA computer policy.

User:

Signature

Date

Supervisor or Office Manager or Contracting Representative:

Printed Name

Signature

Date

Attachment M

**U.S. DEPARTMENT OF AGRICULTURE
NATURAL RESOURCES CONSERVATION SERVICE
NRCS-IRM-03**

**Information System Security
Request for User Access to ITS Resources**

Type of Request:		New/Existing (Select "Type of User" Below)		Delete Access (Permanently Deletes User)		Date of Request:	
Part I (Completed by Supervisor/Office Manager/COR/COTR)							
Employee/User Name: (First, Middle, Last):			Nickname/Preferred Name:			Generation: (Jr, Sr, II, III...)	
Position Title:		Reporting/Termination Date:		E-mail:		Phone:	
NRCS Site Names Finder (Site ID, Office ID): http://nrcs-security.sc.egov.usda.gov/itresources/documents/sitenames.xlsx							
Site ID:		Office ID:		City:		State:	
Affiliate/Company or Organization Name:							
Access Required: (Note: Access to NRCS applications (e.g., ProTracts/Fund Manager) is not requested through this process. Refer to the Information Technology Assistance SOP: http://directives.sc.egov.usda.gov/OpenNonWebContent.aspx?content=18456.wba)							
Type of User:		New Federal		New Affiliate		New Contractor	
		Existing Federal		Existing Affiliate		Existing Contractor	
Active Directory Account?							
Yes with Email		Yes without Email					
Active Directory Removal		Other (Explain in Comments)		No Action			
Specify Email address if different than office location:							
Specify if User needs to be added to any email distribution groups such as "All CEDs" or others:							
Install Hardware? (Laptop/Desktop - Describe needed installation in "Detail/Comments" Section)							
Check box ONLY if User needs a Telephone (Land Line):							
Check box ONLY if User needs a Blackberry?							
<i>(ISSPOCs – If this box is checked then you must include notes in the "Details/Comments" section that user needs a Blackberry and at least one box under "Active Directory" must be checked)</i>							
Is this a Name Change Request? (Provide Information):							
Is this a Phone # Update Request? (Provide Information):							
Is the User Transferring to a different Agency? [Select New Agency - FAS, FSA, ITS, NITC, or RD]:							
Note to ISSPOC's only: Currently you may not be able to select the new agency the user will be transferring to in the SAAR ticket. If this is the case you must select USDA-NRCS in this field and then note the agency the user will be transferring to in the Details/Comments section (e.g., User Transferring to [Agency]).							
Is this a Location Update Request? http://nrcs-security.sc.egov.usda.gov/itresources/documents/sitenames.xlsx							
Place updated location below:							
Site ID		Office ID					
City		State					

Agency Account Request (Please provide all additional information for these requests in the Details/Comments Section):

End User VPN/Dialup Access (<u>must</u> provide justification)	Add	Delete
SAAR POC Account Entitlement (Use the "ISSPOC_DCCAC Request" form and email to nrcsaccesscontrol@ftc.usda.gov)		
Remedy Support Groups (provide group information)	Add	Delete
SafeBoot (<u>must</u> provide justification for exemption)	Re-Enable	Request Exemption
Local Workstation Admin (<u>must</u> provide justification)	Add Rights	Delete Rights
Share Drive Permissions (provide information)	Add Permissions	Remove Permissions
Other Elevated Privileges (<u>must</u> provide justification)	Add	Delete
Toolkit User Group Membership	Add	Remove

(If ToolKit Access is checked – Select "Other Elevated Privileges" in Remedy and state in the Details/Comments Section that Toolkit Access is needed.)

Details/Comments (additional justification and/or information):**Verification of Least Privilege / Need to Know**

I certify that this user requires account access as requested in the performance of his/her job function.

Signature of Supervisor/Office Manager/Contracting Rep:

Date completed:

Part II (Completed by Human Resources Staff)

EmpowHR or Affiliate or NEIS ID (required for email access):

Type of Investigation (NAC, NACI...):

Date Paperwork Received:

Date of Initiation:

Clearance Level: (None, Secret, etc.)

Date Investigation Completed:

HR Manager/Representative Signature:

Date completed:

Part III (Completed by Center/State Training Officer or Designee)

Completed Information Security Awareness and Rules of Behavior Training:

If No or Unknown, must provide details:

Yes

No

Unknown

Training Officer or Designee Signature:

Date completed:

Part IV (Completed by ISSPOC and attach form to the SAAR ticket)

ISSPOC's Signature:

Date completed:

Summary of Comments on NRCS Request for User Access to ITS Resources

Page: 1

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:03:00 AM
New/Existing - For New/Existing Users ALL parts of the IRM3 need to be completed and signed.

Also use this for Disabling accounts and transfers/moves.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:20:37 AM
Delete Access - Only Part 1 and Part 4 of the IRM 3 need to be complete.

THIS TYPE OF REQUEST IS TO COMPLETELY DELETE A USERS ACCESS. DO NOT USE FOR TRANSFERING EMPLOYEES. USE NEW/EXISTING.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:50:14 AM
Site ID, Office ID, City, and State need to be completed for New Users ONLY. Use the link by NRCS Site Names Finder to find the correct info for this section.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:21:14 AM
Regarding ALL sections in access required - ONLY CHECK/Complete those sections for access that is needed.(If they are an existing employee, don't check access they ALREADY have - Only access that needs to be added).

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:49:47 AM
Active Directory Account - 1 of these boxes OTHER than "No Action" needs to be checked if anything is needed from the group that handles Active Directory Accounts

"No Action" Does just that - DOES not generate a CRQ

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:49:42 AM
Specify Email if Different - This DOES NOT include transfers This section is only for a user who works for a location that is different that where he is physically located and wants an email address with that location.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:49:32 AM
Email Distro Groups - There are certain distro groups that users are automatically added to as part of the account creation.

This section is only for non generic groups that may be specific to users duties

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:49:29 AM
Install Hardware - Explain in Details/Comments section what type of hardware is needed.

E.G.
Laptop - special software needed, etc.
Desktop

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:49:24 AM
Blackberry

If the user needs a blackberry you will need to state it in the Details/Comments Section. Also at least one of the boxes under Active Directory needs to be checked. (May already have something checked if it's for a new user)

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:49:21 AM
Name Change - If you need to submit a name change request due to marriage or any other reason, you ONLY need to complete this section. When you enter info in this section it generates 3 CRQ's, 1 for AD/Email, 1 for Remedy, and 1 for Webfarm.

If the request is only for a name change, you do NOT need to check anything in the active directory section.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:49:18 AM
Phone # Update - Updating info here generates CRQ's to update the GAL and Remedy.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:49:15 AM
Transferring to Different Agency -

If they are ITS supported then Select which agency they are going to here.

ISSPOC's - In the Remedy request you will select NRCS here and then in the notes state the actual agency they are transferring too.

If they are transferring to an non ITS supported agency that is not listed to the left - then you must submit a delete ticket

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:49:12 AM
Location Update Request

This section is only for a user who is moving locations. The losing location MUST enter a IRM3/Remedy ticket FIRST - This will be to remove their access at that location and to update their location in Remedy. Once the users location in Remedy has been updated then the gaining location can enter an IRM3/Remedy ticket to give them access at the new location.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:49:08 AM

Agency Account Request Section -

Only Check the Access that needs to be ADDED or that needs to be REMOVED.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:36:23 AM

VPN Access is for users who Telework or need to have access during Travel. If need this access select "Add" and provide justification. If you don't need this access, simply ignore (Don't check ANYTHING). Selecting "Delete" will remove VPN access if the user has it.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:36:40 AM

SAAR POC This access is for ISSPOC's Only. Should NEVER be checked in REMEDY!

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:37:00 AM

Remedy Support Groups - This type of access is only for Remedy Help Desk - You Should NEVER need to request this type of access but if you do, then please provide a detailed justification as to why.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:38:14 AM

Safeboot - Users need to explain why they need to be exempt from having safeboot on their system.

If you are unsure about this then it's best to leave blank. The user/manager should have a detailed reason why this is not needed.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:38:34 AM

Local Admin - We need a good justification as to why rights are needed in the Details/Comments section. If they don't need it - don't check either box.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:38:52 AM

Shared Drive - If you check Add or Remove access to Shared Drive - You need to put in the Details/Comments section what Drive they need access to.

This does NOT include standard shared drive access that is included with account creation - e.g.- h, s, t (restricted by groups)

Other sites may use different letters.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:39:12 AM

Elevated Privileges - If needed please specify exactly what is needed in Details/Comments. If not needed don't check with box.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:41:20 AM

Toolkit User Group Membership - This section is on the IRM3 Only and NOT in remedy. If this section is checked then you must check "Other Elevated Privileges" in Remedy and specify in the Details/Comments section that user needs to be added to the Toolkit User Group

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:46:43 AM

Details/Comments section - needs to be detailed and provide info to any boxes that have been checked above that require a Justification.

e.g.,

- New Federal Employee
- Shared Drive - Drive//Path
- Local Admin - Needed to install software
- EmpowHR, Affiliate, or NEIS ID
- Add to Toolkit User Group

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:47:28 AM

Part 2 This section needs to be completed for EVERY request EXCEPT Deletes.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:48:03 AM

The EmpowHR, Affiliate, or NEIS ID needs to be placed in the Details/Comments Section of the Remedy ticket by the ISSPOC.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:47:36 AM

Part 3 This section needs to be completed for EVERY request EXCEPT Deletes.

Author: Lee.Espinoza Subject: Sticky Note Date: 3/2/2011 11:48:18 AM

Needs to be signed and dated by ISSPOC and also attached to the Remedy ticket. (Scanned with hard signatures or just attached with Digital Signatures.)

Declaration for Federal Employment

50306-101

INSTRUCTIONS

The information collected on this form is used to determine your acceptability for Federal employment and your enrollment status in the Government's Life Insurance program. You may be asked to complete this form at any time during the hiring process.

Follow instructions that the agency provides. If you are selected, you will be asked to update your responses on this form and on other materials submitted during the application process and then to recertify that your answers are true before you are appointed.

Your Social Security Number is needed to keep our records accurate, because people may have the same name and birthdate. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records. Giving us your SSN or any other information is voluntary. However,

if you do not give us your SSN or any other information requested, we cannot process your application. Incomplete addresses and ZIP Codes may also slow processing.

You must answer all questions truthfully and completely. A false statement on any part of this declaration or attached forms or sheets may be grounds for not hiring you, or for firing you after you begin work. Also, you may be punished by fine or imprisonment (U.S. Code, title 18, section 1001).

Either type your responses to this form or print clearly in dark ink. If you need additional space, attach letter-size sheets (8.5" X 11"), including your name, Social Security Number, and item number on each sheet. It is recommended that you keep a photocopy of your completed form for your records.

Declaration for Federal Employment

GENERAL INFORMATION

1 FULL NAME



2 SOCIAL SECURITY NUMBER



3 PLACE OF BIRTH (Include City and State or Country)



4 DATE OF BIRTH (MM/DD/YY)



5 OTHER NAMES EVER USED (For example, maiden name, nickname, etc.)



6 PHONE NUMBERS (Include Area Codes)

DAY

NIGHT

MILITARY SERVICE

7 Have you served in the United States Military Service? *If your only active duty was training in the Reserves or National Guard, answer "NO".*

Yes	No

If you answered "YES", list the branch, dates (MM/DD/YY), and type of discharge for all active duty military service.

BRANCH	FROM	TO	TYPE OF DISCHARGE

BACKGROUND INFORMATION

For all questions, provide all additional requested information under item 15 or on attached sheets. The circumstances of each event you list will be considered. However, in most cases you can still be considered for Federal jobs.

For questions 8, 9, and 10, your answers should include convictions resulting from a plea of nolo contendere (*no contest*), but omit (1) traffic fines of \$300 or less, (2) any violation of law committed before your 16th birthday, (3) any violation of law committed before your 18th birthday if finally decided in juvenile court or under a Youth Offender law, (4) any conviction set aside under the Federal Youth Corrections Act or similar State law, and (5) any conviction whose record was expunged under Federal or State law.

8 During the last 10 years, have you been convicted, been imprisoned, been on probation, or been on parole? (Includes felonies, firearms or explosives violations, misdemeanors, and all other offenses.) *If "Yes", use item 15 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved.*

Yes	No

9 Have you been convicted by a military court-martial in the past 10 years? (If no military service, answer "NO".) *If "Yes", use item 15 to provide the date, explanation of the violation, place of occurrence, and the name and address of the military authority or court involved.*

--	--

10 Are you now under charges for any violation of law? *If "Yes", use item 15 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved.*

--	--

11 During the last 5 years, were you fired from any job for any reason, did you quit after being told that you would be fired, did you leave any job by mutual agreement because of specific problems, or were you debarred from Federal employment by the Office of Personnel Management? *If "Yes", use item 15 to provide the date, an explanation of the problem and reason for leaving, and the employer's name and address.*

--	--

12 Are you delinquent on any Federal debt? (Includes delinquencies arising from Federal taxes, loans, overpayment of benefits, and other debts to the U.S. Government, plus defaults of Federally guaranteed or insured loans such as student and home mortgage loans.) *If "Yes", use item 15 to provide the type, length, and amount of the delinquency or default, and steps that you are taking to correct the error or repay the debt.*

--	--

ADDITIONAL QUESTIONS

13 Do any of your relatives work for the agency or organization to which you are submitting this form? (Includes father, mother, husband, wife, son, daughter, brother, sister, uncle, aunt, first cousin, nephew, niece, father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, sister-in-law, stepfather, stepmother, stepson, stepdaughter, stepbrother, stepsister, half brother, and half sister.) *If "Yes", use item 15 to provide the name, relationship, and the Department, Agency, or Branch of the Armed Forces for which your relative works.*

Yes	No

14 Do you receive, or have you ever applied for, retirement pay, pension, or other pay based on military, Federal civilian, or District of Columbia Government service?

--	--

CONTINUATION SPACE / AGENCY OPTIONAL QUESTIONS

15 Provide details requested in items 8 through 13 and 17c in the continuation space below or on attached sheets. Be sure to identify attached sheets with your name, Social Security Number, and item number, and to include ZIP Codes in all addresses. If any questions are printed below, please answer as instructed (these questions are specific to your position, and your agency is authorized to ask them).

CERTIFICATIONS / ADDITIONAL QUESTION

APPLICANT: If you are applying for a position and have not yet been selected, Carefully review your answers on this form and any attached sheets. When this form and all attached materials are accurate, complete item 16/16a.

APPOINTEE: If you are being appointed, Carefully review your answers on this form and any attached sheets, including any other application materials that your agency has attached to this form. If any information requires correction to be accurate as of the date you are signing, make changes on this form or the attachments and/or provide updated information on additional sheets, initialing and dating all changes and additions. When this form and all attached materials are accurate, complete item 16/16b and answer item 17.

16 I certify that, to the best of my knowledge and belief, all of the information on and attached to this Declaration for Federal Employment, including any attached application materials, is true, correct, complete, and made in good faith. **I understand** that a false or fraudulent answer to any question on any part of this declaration or its attachments may be grounds for not hiring me, or for firing me after I begin work, and may be punishable by fine or imprisonment. **I understand** that any information I give may be investigated for purposes of determining eligibility for Federal employment as allowed by law or Presidential order. **I consent** to the release of information about my ability and fitness for Federal employment by *employers, schools, law enforcement agencies, and other individuals and organizations to investigators, personnel specialists, and other authorized employees of the Federal Government.* **I understand** that for financial or lending institutions, medical institutions, hospitals, health care professionals, and some other sources of information, a separate specific release may be needed, and I may be contacted for such a release at a later date.

16a Applicant's Signature ▶
(Sign in ink)

Date ▶

16b Appointee's Signature ▶
(Sign in ink)

Date ▶

APPOINTING OFFICER: Enter Date of Appointment or Conversion

17 Appointee Only (Respond only if you have been employed by the Federal Government before): Your elections of life insurance during previous Federal employment may affect your eligibility for life insurance during your new appointment. These questions are asked to help your personnel office make a correct determination.

17a When did you leave your last Federal job? -----

17b When you worked for the Federal Government the last time, did you waive Basic Life Insurance or any type of optional life insurance? -----

17c If you answered "Yes" to item 17b, did you later cancel the waiver(s)? *If your answer to item 17c is "No," use item 15 to identify the type(s) of insurance for which waivers were not cancelled.* -----

Date (MM/DD/YY)		
Yes	No	Don't Know

PRIVACY ACT AND PUBLIC BURDEN STATEMENT

The Office of Personnel Management is authorized to request this information under sections 1302, 3301, 3304, and 8716 of title 5 of the U.S. Code. Section 1104 of title 5 allows the Office of Personnel Management to delegate personnel management functions to other Federal agencies. If necessary, and usually in conjunction with another form or forms, this form may be used in conducting an investigation to determine your suitability or your ability to hold a security clearance, and it may be disclosed to authorized officials making similar, subsequent determinations.

Public burden reporting for this collection of information is estimated to vary from 5 to 30 minutes with an average of 15 minutes per response, including time for reviewing instructions, searching existing data sources, gathering the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden, to Reports and Forms Management Officer, U.S. Office of Personnel Management, 1900 E Street, N.W., Washington, D.C. 20415.

ROUTINE USES: Any disclosure of this record or information in this record is in accordance with routine uses found in System Notice OPM/GOVT-1, General Personnel Records. This system allows disclosure of information to training facilities; organizations deciding claims for retirement, insurance, unemployment, or health benefits; officials in litigation or administrative proceeding where the Government is a party; law enforcement agencies concerning a violation of law or regulation; Federal agencies for statistical reports and studies; officials of labor organizations recognized by law in connection with representing employees; Federal agencies or other sources requesting information for Federal agencies in connection with hiring or retaining, security clearance, security or suitability investigations, classifying jobs, contracting, or issuing licenses, grants, or other benefits; public and private organizations, including news media, which grant or publicize employee recognition and awards; the Merit Systems Protection Board, the Office of Special Counsel, the Equal Employment Opportunity Commission, the Federal Labor Relations Authority, the National Archives,

the Federal Acquisitions Institute, and Congressional offices in connection with their official functions; prospective non-Federal employers concerning tenure of employment, civil service status, length of service, and the date and nature of action for separation as shown on the SF 50 (or authorized exception) of a specifically identified individual; requesting organizations or individuals concerning the home address and other relevant information on those who might have contracted an illness or been exposed to a health hazard; authorized Federal and non-Federal agencies for use in computer matching; spouses or dependent children asking whether the employee has changed from a self-and-family to a self-only health benefits enrollment; individuals working on a contract, service, grant, cooperative agreement, or job for the Federal government; non-agency members of an agency's performance or other panel; and agency-appointed representatives of employees concerning information issued to the employee about fitness-for-duty or agency-filed disability retirement procedures.



The NRCS Sponsor has determined by agency Risk Assessment that a performing Earth Team Volunteer requires a LincPass. The information collected on this Personal Identity Information (PII) sheet is required for LincPass sponsorship. This information is to be collected and transmitted in accordance with the Privacy Act of 1974 (5 U.S.C. Section 552a). Furnishing this information is voluntary; however, failure to furnish correct, complete information will result in the withholding of your LincPass. For details on the Privacy Act of 1974, visit this Web site: <http://www.justice.gov/opcl/privstat.htm>

Instructions: Enter the information below. Enter applicant's complete name and address as it appears on their government-issued ID, such as a driver's license or passport. If the information doesn't match, the non-employee will encounter problems during the enrollment process and may have to reapply.

NRCS Office Name:
Earth Team Volunteer Coordinator Name: <i>State Volunteer Coordinator Name</i>
Earth Team Volunteer Coordinator Business Phone:
Applicant Name: <i>First, Middle (if any), Last, Suffix (if any):</i>
Applicant Social Security Number <i>(xxx-xx-xxxx):</i>
Applicant Date of Birth <i>(mm/dd/yyyy):</i>
Applicant Place of Birth <i>(City/State. If outside U.S., enter City/Country.):</i>
Applicant Business Email <i>(This is for enrollment notification. If the applicant does not have a business email address, enter the address of the person who will manage enrollment activities, e.g. Security Officer, Supervisor, or Human Resources Manager.):</i>
Applicant Business Phone:
Applicant Country of Citizenship <i>(Enter the applicant's country of citizenship):</i>
Applicant Non-Employee Type <i>(Enter one of the following: Contractor, Volunteer, Soil and Water Conservation District, Intern, or Other Non-Federal Employee.):</i>



Applicant Home Address (*Enter the applicant's home address. Remember that it is strongly recommended that you enter the applicant's address as shown on their government-issued ID, such as a driver's license or passport.*):

Applicant Work Address (*Enter the applicant's work address*):

Please hand carry or send via locally-secured fax to:
[Enter Security Officer/Data Entry Personnel Contact Information]

Attachment P

ELECTRONIC QUESTIONNAIRES FOR INVESTIGATIONS PROCESSING

e-QIP

Version 2.00

Quick Reference Guide for e-QIP Applicants

- If using **AOL**, open a separate window in Internet Explorer (outside AOL) and set the options for Active Scripting and TLS 1.0 following the instructions above; or directly within AOL, go to the top menu in AOL, then:
 - Select **SETTINGS**
 - Select **INTERNET PROPERTIES**
 - Under **RELATED SETTINGS**, select **INTERNET EXPLORER SETTINGS**, then the **ADVANCED** tab
 - Scroll down to **SECURITY**
 - Check the box to enable **TLS 1.0**
 - Click the **APPLY** button
 - Select the **SECURITY** tab and **CUSTOM LEVEL**
 - Check the box to enable **ACTIVE SCRIPTING** and the **OK** button to save
 - Click **SAVE** in the AOL Browser Settings box

If you are using **Mozilla Firefox**, you must have at least version 0.9.4. Although security settings may already be defaulted to the proper values, you should verify as follows:

- Select **TOOLS**
 - Select **OPTIONS**
 - Select **ADVANCED**
 - Select the **ENCRYPTION** tab
 - Under "Protocols", check the boxes to enable **SSL 3.0** and **TLS 1.0**
- For **Mozilla Firefox** users to verify that they are enabled to use cookies, go to the browser's toolbar and verify in the following order:
- Select **TOOLS**
 - Select **OPTIONS**
 - Select **PRIVACY**
 - Under the "Cookies" section, ensure that **ACCEPT COOKIES FROM SITES** is checked

e-QIP is also compatible with **Netscape Navigator** 6.1 and newer. Settings for the latest version can be made following the same instructions above for Mozilla Firefox.

If using **JAWS** screen-reading software, please note that **JAWS** requires the use of Internet Explorer, version 5.5 or newer.

Getting Started

1. Start your internet browser and enter the following URL, website address:
www.opm.gov/e-qip/
2. The e-QIP Gateway Page will appear. Scroll down and click the button labeled **ENTER e-QIP APPLICANT SITE**.
3. A "browser checker" utility will automatically run and test your computer for e-QIP compatibility. Click the **CONTINUE** button to proceed to the application. (If you receive the error message "**Page Cannot Be Displayed**", please follow the instructions to enable TLS 1.0 on the "Testing Your Web Browser for Compatibility" page.)
4. A Security Alert box may appear, asking "Do you want to proceed??" Click the **YES** button with the mouse, or type <ALT Y> to continue.
5. The e-QIP Welcome Screen will appear. Enter your Social Security Number in the text entry boxes, and click the **SUBMIT** button to logon to the e-QIP applicant site.
6. Answer the three (3) default Golden Questions and then you may create new Golden Questions and Answers on the next page (please see the applicable section inside this brochure for further information).
7. Click the highlighted link that says: **Enter Your Data**.
8. Complete the form questions and save as instructed. Validation of your data will occur after every screen save.
9. Be sure to **CERTIFY** and **RELEASE** your form when complete.
10. Print out the release forms and certification for your signature. These signature forms need to be returned to your hiring agency. You may also print out an archival copy for your own records. (If you are having difficulty opening the forms to print, right click the link, choose **SAVE AS**, and then

save the file on your computer. Open up the Adobe Acrobat reader program separately in its own window (not through the browser), and then open the file you saved in order to print it out successfully.)

Choosing Your Golden Questions/Answers

It is **YOUR RESPONSIBILITY** to provide and remember Golden Questions unique to you. Golden Questions enable e-QIP to verify your identity. Create a combination of Golden Questions that only you can know the correct answers to in order to assure that no one can attempt to impersonate you on the e-QIP system. Remember that it may be 5 years before you return to the e-QIP system for a future reinvestigation. Please contact your sponsoring agency if you are having difficulty with your login.

Entering Your Golden Questions/Answers

After you have selected your set of Golden Questions/Answers, enter each Question under a "Question" header and enter the corresponding Answer under the "Answer" block directly under that question. You must provide a non-blank answer for each question you provide, and vice versa. You must provide three Golden Questions.

It is **your responsibility** to protect the answers to your Golden Questions. Golden Answers are your "password" to the e-QIP system. The text entry fields for Golden Answers are not password protected to allow for more accurate entry of your answers. Asterisks automatically mask Golden Answers, but if you choose, you can view your answers while typing them by clicking the **ALLOW ME TO SEE MY GOLDEN ANSWERS** checkbox. Do not allow someone to see your computer screen while your answers are on the screen. If someone acquires your answers, they will be able to logon to the e-QIP system under your identity, allowing them to access your personal data.



Questions? Please contact:

U.S. Office of Personnel Management
Federal Investigative Services Division
1900 E Street NW, Room 2H31
Washington, DC 20415
ATTN: OPM e-QIP Project Manager
E-mail: e-QIP@opm.gov

Brochure revised February 2008

Entering Your Data

First Time Data Entry: Prior to entering data for the first time, read the instructions on the "Form Completion Instructions" screen. Indicate that you have read and understand the document by clicking the corresponding button. For the SF-86 form, you will also be shown a disclaimer screen that provides additional instructions required by Executive Order 12968. You will need to indicate that you have read and understand the additional instructions by clicking the corresponding button.

Question Navigation: You may use the Navigation pull-down menu to go to any question, in any order, by selecting the item and clicking **GO**. The navigation menu is located in the top right-hand corner of the screen.

Errors and Warnings: After clicking **SAVE**, if the system displays the same screen with "Validation Results" listed at the top, you must correct the data you have just entered. You will only get validation messages if you have not answered a question appropriately.

For validation "**Error**" messages, you may correct your data by scrolling to the appropriate field and editing. After making corrections, click the **SAVE** button at the bottom of that page to save your changes.

For validation "**Warning**" messages, you may either provide the requested information or check the box for **IDO NOT KNOW THE REQUESTED INFORMATION**. In some cases an additional explanation is required if the check box is used for not knowing the information. After choosing an action, click the **SAVE** button to save your changes.

For validation "Error" and "Warning" messages, you may also choose to click the **SAVE/CONTINUE** button. If you click **SAVE/CONTINUE**, you may advance to the next question screen and correct the information at a later time prior to the final submission of your form.

If you make a mistake and want to start over on a given screen, click on the **RESET THIS SCREEN** button at any time prior to clicking the **SAVE** button. This clears all of the answers on that page.

When you are finished and ready to proceed, click the **SAVE** button. Upon clicking **SAVE**, your information will be submitted and you will proceed to the next screen.

Displaying Your Data

When you are ready to display and/or print your personal information that has been entered into e-QIP, select the "Display" link on the top banner (located in the upper left-hand corner).

By selecting "Display", a new browser window will appear. This window will contain an HTML formatted file which will display on the screen all the data that has been entered up to that point. If desired, you can print the displayed data by first selecting "File", then "Print" from the new browser window.

Validating Your Data

Although the e-QIP system will automatically validate your data after every screen save, you may also do a manual validation. To do so, go to the navigation pull-down menu and select **VALIDATE, REVIEW, AND CERTIFY**, then select **GO** to the right of the pull-down menu, and the system will take you to that screen.

The validation results may show Errors and/or Warnings that need to be corrected. Read the validation results and the associated errors. To correct your answers, use the navigation pull-down menu to go to the question that needs to be edited, make the necessary changes, and click the **SAVE** button.

Listing Expected Attachments

You may create a list of attachments that you expect to provide to your employing agency. Ask

your sponsoring agency if you are not sure what attachments you are required to provide.

To create your list of expected attachments, go to the navigation pull-down menu and select **EXPECTED ATTACHMENTS**. Then select **GO** to the right of the pull-down menu, and the system will take you to that screen. (You will be shown this automatically if you complete your form in sequence. If you choose to skip from question to question, you will need to select this command manually).

This screen allows you to create, delete, and/or edit a list of expected attachments that you may send with your request. Then you must mail, drop off, or fax your attachments to your agency, along with your signature forms, per your agency's instructions.

Certifying Your Data

When you have completed all the questions on the form and are ready to submit, select the **VALIDATE, REVIEW, AND CERTIFY** command from the Navigation menu at the top of the screen and click **GO**. If the message displayed is "Validation found no errors or unsatisfied warnings", click the **CONTINUE** button to proceed. The next screen will request a final review of your data with another **CONTINUE** button to proceed.

The following screen will have a **CERTIFY INVESTIGATION REQUEST** button. After certification, **YOU WILL NO LONGER BE ABLE TO MAKE ANY CHANGES** - your answers to the questionnaire will be locked and unavailable for editing.

Final release of your request is in three steps on the "Release Investigation Request" screen.

1. First, select **Display the Archival Copy of this Investigation Request for Printing** to generate a PDF copy of your form data to print and/or save for your records.
2. Second, select **Display the Signature Form(s) for Printing** to generate the release forms and

certification statement. Your computer must have Adobe Acrobat in order to view these PDF files. This free software download is available at:

www.adobe.com/products/acrobat/readstep2.html

You are required to print the release form(s) and the certification statement. If you do not have a printer, you should consult your sponsoring agency and ask for assistance. After printing, please sign them (preferably in black ink) and return the originals to your agency.

3. The third and final step is clicking the **Release Request/Transmit to Agency** button. After you have successfully certified your form and released it to your agency, you cannot change your data or log back into the system. However, the next time you need access to e-QIP, such as for a future reinvestigation, most of your data will repopulate the e-QIP form, eliminating the need to re-enter all of your data.

Web Browser Requirements

If using **Microsoft Internet Explorer (IE)**, you must have version 5.5 or later, with Service Pack 2. Internet Options for IE should be set as follows:

- Select **TOOLS**
- Select **INTERNET OPTIONS**
- Select the tab labeled **SECURITY**
- Select **CUSTOM LEVEL**
- Check the box to enable **ACTIVE SCRIPTING** and the **OK** button to save

To enable TLS 1.0 in IE, on the top menu:

- Select **TOOLS**
- Select **INTERNET OPTIONS**
- Select the tab labeled **ADVANCED**
- Scroll down to the **SECURITY** section
- Check the box to enable **TLS 1.0**
- Click the **OK** button to save

**NATURAL RESOURCES CONSERVATION SERVICE (NRCS)
UNITED STATES DEPARTMENT OF AGRICULTURE (USDA)**

ACKNOWLEDGMENT OF SECTION 1619 COMPLIANCE

Purpose and Background

The purpose of this Acknowledgment of Section 1619 compliance (hereinafter “Acknowledgment”) is to require acknowledgment by *[replace with the name of the individual/organization]* of the requirements of Section 1619 of the Food, Conservation, and Energy Act of 2008 (the 2008 Farm Bill), which prohibits disclosure of certain information by the Department of Agriculture (USDA) and its cooperators. *[replace with the name of the individual or organization]* assists NRCS in the delivery of conservation-related services (for example, services that sustain agricultural productivity, improve environmental quality, reduce soil erosion, enhance water supplies, improve water quality, increase wildlife habitat, and reduce damages caused by floods and other natural disasters) or with monitoring, assessing, or evaluating of conservation benefits from USDA conservation programs under a *[replace with specific type of “master” agreement used; for example,, a cooperative agreement, contribution agreement, etc.]*. Those individuals or organizations (governmental or nongovernmental) that assist NRCS with providing conservation-related services are known as NRCS Conservation Cooperators.

NRCS Conservation Cooperator

As an NRCS Conservation Cooperator, *[replace with the name of the individual or organization]* is authorized access to otherwise-protected agricultural information. Such protected information must be strictly limited to only that information necessary for *[replace with the name of the individual or organization]* *[choose to provide conservation related services or to perform monitoring, assessing, or evaluating of conservation benefits]*. Disclosure to *[replace with the name of the individual or organization]* can include receiving the protected information either 1) directly from NRCS; 2) directly from the producer or owner as part of the process required to enable a producer or owner to participate in a USDA program; or 3) in another manner with the producer’s permission.

Section 1619 of the 2008 Farm Bill

Section 1619 of the Food, Conservation, and Energy Act of 2008 (Exhibit 1) (hereinafter “section 1619” provides that USDA, or any “contractor or cooperator” of USDA, “shall not disclose—(A) information provided by an agricultural producer or owner of agricultural land concerning the agricultural operation, farming or conservation practices, or the land itself, in order to participate in the programs of the Department; or (B) geospatial information otherwise maintained by the Secretary about agricultural land or operations for which information described in subparagraph (A) is provided.” USDA may disclose protected information to a USDA cooperator when such cooperator is “providing technical or financial assistance with respect to the agricultural operation, agricultural land, or farming or conservation practices” if USDA determines that the protected information will not be subsequently disclosed, except in accordance with the exceptions contained in Section 1619. *[Replace with the name of the individual or organization]* is a “contractor or cooperator” of USDA within the meaning of Section 1619. Accordingly, *[replace with the name of the individual or organization]* may not subsequently disclose any information protected by section 1619. By signature on this

Acknowledgment, [*replace with the name of the individual or organization*] is certifying future compliance with the statutory obligations under Section 1619. Upon execution of this Acknowledgment, NRCS may continue to provide to [*replace with the name of the individual or organization*] the protected information provided under [*replace with specific type of “master” agreement used; for example, a cooperative agreement, contribution agreement, etc.*].

Responsibilities

[*Replace with the name of the individual or organization*] (hereinafter the “Conservation Cooperator”) certifies that:

- Signature on this Acknowledgment indicates acknowledgment and understanding that the Conservation Cooperator is legally bound by Federal statute to comply with the provisions of Section 1619 and that the Conservation Cooperator will not subsequently disclose information protected by section 1619 to any individual or organization that is not directly covered by this Acknowledgment. Any such subsequent disclosure of the protected information (except as permitted under Section 1619) will be considered a violation of Section 1619. The Conservation Cooperator will be held responsible should disclosure of the protected information occur.
- Signature on this Acknowledgment legally binds every owner, manager, supervisor, employee, contractor, agent, and representative of the Conservation Cooperator to comply with the provisions in Section 1619. The Conservation Cooperator must consult with NRCS prior to providing protected information to an entity or individual outside of the Conservation Cooperator and as necessary to implement the program to ensure that such release is permissible.
- The Conservation Cooperator will use the protected information only to perform work that is directly connected to [*choose* provide conservation related services *or* perform monitoring, assessing, or evaluating conservation benefits]. Use of the protected information to perform work that is not directly connected to [*choose* provide conservation related services *or* perform monitoring, assessing, or evaluating conservation benefits] is expressly prohibited.
- The Conservation Cooperator must internally restrict access to the protected information to only those individuals who have a demonstrated need to know the protected information in order to [*choose* provide conservation related services *or* perform monitoring, assessing, or evaluation of conservation benefits].
- The provisions in Section 1619 are continuing obligations. Even when the Conservation Cooperator is no longer an NRCS Conservation Cooperator, or when individuals currently affiliated with the Conservation Cooperator become no longer so affiliated, every person having been provided access to the protected information will continue to be legally bound to comply with the provisions of this Acknowledgment.
- The Conservation Cooperator must notify all managers, supervisors, employees, contractors, agents, and representatives about this Acknowledgment and the requirements of Section 1619. For the duration of this Acknowledgment, notifications about the existence of this Acknowledgment must be made to those individuals who are new to the

organization and periodic notifications must be sent throughout the organization (as well as to all contractors and agents) to remind all about the ongoing and continuing requirements.

- When the Conservation Cooperator is unsure whether particular information is covered or protected by Section 1619, the Conservation Cooperator must consult with NRCS to determine whether the information must be withheld.
- This Acknowledgment is nontransferable and may not be bought, sold, traded, assigned, extended to, or given free of charge to any other individual or organization not directly covered by this Acknowledgment.
- Use of the protected information for any purpose is expressly prohibited when an individual or organization is no longer an NRCS Conservation Cooperator. When the Conservation Cooperator is no longer an NRCS Conservation Cooperator, any protected information provided under this Acknowledgment must be immediately destroyed or returned to NRCS. The Conservation Cooperator must provide to NRCS written certification that the protected information (paper copy, electronic copy, or both) has been properly destroyed, removed from any electronic storage media, or both.
- *[If the cooperator is a State governmental employee, contractor, or representative or a State agency - remove this bullet if not applicable]* The State's "sunshine law," "open records act" or other version of the Freedom of Information Act is superseded by section 1619 under the Supremacy Clause of the U.S. Constitution. Accordingly, information protected from disclosure by section 1619 must not be released under such State laws.
- *Note: If the Secretary of Agriculture can not determine that the protected information will be properly withheld by a State governmental agency, (for example., State policy indicating that public disclosure of information will not be required for records that are specifically required by the Federal Government to be kept confidential), then section 1619 prohibits the disclosure of the protected information to the State governmental agency. Acknowledgement of this provision by a State agency/employee's signature confirms a presumption for that determination. Conversely, failure or refusal to sign undermines the determination and prevents information sharing. Remove this text from the final Acknowledgment.*

Protected Information

An example of the type of information prohibited by disclosure under Section 1619 includes, but is **not limited to**, the following:

- State identification and county number (where reported and where located).
- Producer or landowner name, business full address, phone number, Social Security Number, and similar personal identifying information.
- Farm, tract, field, and contract numbers.
- Production shares and share of acres for each Farm Serial Number (FSN) field.
- Acreage information, including crop codes.
- All attributes for Common Land Units (CLUs) in USDA's Geospatial Information System

- Any photographic, map, or geospatial data that, when combined with other maps, can be used to identify a landowner.
- Location of conservation practices.

Section 1619 allows disclosure of “payment information (including payment information and the names and addresses of recipients of payments) under any Department program *that is otherwise authorized by law*” (emphasis added). The names and payment information of producers generally may be provided to the public; however the Conservation Cooperator shall consult with NRCS if there is any uncertainty as to the provision of such information.

Section 1619 also allows disclosure of otherwise protected information if “the information has been transformed into a statistical or aggregate form without naming any—(i) individual owner, operator, or producer; or (ii) specific data gathering cite.” The Conservation Cooperator must consult with NRCS as to whether specific information falls within this exception prior to relying on this exception.

Violations

The Conservation Cooperator will be held responsible for violations of this Acknowledgment and Section 1619. A violation of this Acknowledgment by the Conservation Cooperator may result in action by NRCS, including termination of the underlying [*replace with specific type of “master” agreement used; for example, a cooperative agreement, contribution agreement, etc.*].

Effective Period

This Acknowledgment will be in effect on the date of the final signature and continues until NRCS notifies the Conservation Cooperator that the Acknowledgment is no longer required based on changes in applicable Federal law.

Signature of the NRCS Conservation Cooperator and the Date Signed

[**Signature Block for the NRCS Conservation Cooperator*]

Executed this ____ day of _____, 20__

** When signature is made on behalf of an organization, this must be an official within the organization with the authority to legally bind the entire organization to comply with the provisions in Section 1619. Remove this text from the final Acknowledgment.*

SEC. 1619.
INFORMATION
GATHERING.

(a) GEOSPATIAL SYSTEMS—The Secretary shall ensure that all the geospatial data of the agencies of the Department of Agriculture are portable and standardized.

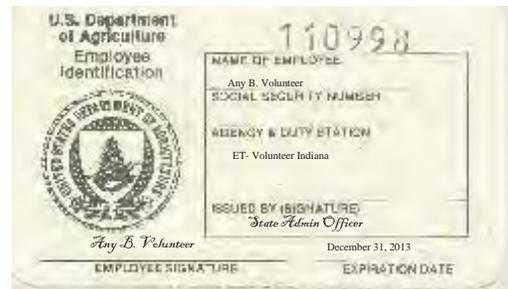
(b) LIMITATION ON DISCLOSURES—

Attachment R

United States Department of Agriculture



Natural Resources Conservation Service
6013 Lakeside Blvd.
Indianapolis, IN 46278



DATE: _____

SUBJECT: PER – Safety and Health – Driver’s Licensing Requirement

TO: Employee

FILE CODE: 360-17-12

To request permission to drive a government owned vehicle, please provide us with the following information:

- 1. I am an (NRCS employee, district employee, state employee, volunteer, other EarthTeam Volunteer). Please circle or write in appropriate category.
2. Your current valid state driver’s license number and state issued
3. List any suspensions or revocations of your state driver’s license or agency driving authorization within the past 5 years
4. List any arrests or summonses for violation of motor vehicle laws, and convictions, if any (do not include non-moving violations)
5. Any motor vehicle accidents within the past 5 years? If yes, please give date and brief description of what occurred.

The following information is needed to issue you a USDA Employee Identification Card.

Name (Please print): _____

Title: _____

Duty Station: _____

Color of Hair/Eyes: _____

Date of Birth: _____

Height/Weight: _____

Employee Signature _____ Date _____

I certify that this employee is capable of safely operating a government owned vehicle.

Supervisor’s Signature _____ Date _____

Agreement on file _____ Approved _____

Area Conservationist (FO) or State Administrative Officer

Attachment S

FOR SALE BY THE SUPERINTENDENT OF DOCUMENTS, US GOVERNMENT PRINTING OFFICE
WASHINGTON, DC 20402 STOCK NO. 048-000-00363-0

Standard Form 1199A
(Rev. June 1987)
Prescribed by Treasury
Department
Treasury Dept. Cir. 1076



SIGN-UP FORM

DIRECTIONS

- To sign up for Direct Deposit, the payee is to read the back of this form and fill in the information requested in Sections 1 and 2. Then take or mail this form to the financial institution. The financial institution will verify the information in Sections 1 and 2, and will complete Section 3. The completed form will be returned to the Government agency identified below.
- A separate form must be completed for each type of payment to be sent by Direct Deposit.
- The claim number and type of payment are printed on Government checks. (See the sample check on the back of this form.) This information is also stated on beneficiary/annuitant award letters and other documents from the Government agency.
- Payees must keep the Government agency informed of any address changes in order to receive important information about benefits and to remain qualified for payments.

SECTION 1 (TO BE COMPLETED BY PAYEE)

A NAME OF PAYEE (<i>last, first, middle initial</i>) Volunteer, Any, A.			D TYPE OF DEPOSITOR ACCOUNT <input checked="" type="checkbox"/> CHECKING <input type="checkbox"/> SAVINGS		
ADDRESS (<i>street, route, P.O. Box, APO/FPO</i>) 1234 Anystreet Blvd.			E DEPOSITOR ACCOUNT NUMBER 9876543		
CITY Anytown	STATE IN	ZIP CODE 12345	F TYPE OF PAYMENT (<i>Check only one</i>)		
TELEPHONE NUMBER AREA CODE (317) 123-4567			<input type="checkbox"/> Social Security <input type="checkbox"/> Fed Salary/Mil. Civilian Pay <input type="checkbox"/> Supplemental Security Income <input type="checkbox"/> Mil. Active _____ <input type="checkbox"/> Railroad Retirement <input type="checkbox"/> Mil. Retire _____ <input type="checkbox"/> Civil Service Retirement (OPM) <input type="checkbox"/> Mil. Survivor _____ <input type="checkbox"/> VA Compensation or Pension <input checked="" type="checkbox"/> Other _____ <div style="text-align: right; font-size: small;">(<i>specify</i>)</div>		
B NAME OF PERSON(S) ENTITLED TO PAYMENT			G THIS BOX FOR ALLOTMENT OF PAYMENT ONLY (<i>if applicable</i>)		
C CLAIM OR PAYROLL ID NUMBER Prefix 123456789 (Social Security #) Suffix			TYPE		AMOUNT
PAYEE/JOINT PAYEE CERTIFICATION I certify that I am entitled to the payment identified above, and that I have read and understood the back of this form. In signing this form, I authorize my payment to be sent to the financial institution named below to be deposited to the designated account.			JOINT ACCOUNT HOLDERS' CERTIFICATION (<i>optional</i>) I certify that I have read and understood the back of this form, including the SPECIAL NOTICE TO JOINT ACCOUNT HOLDERS.		
SIGNATURE Any A. Volunteer		DATE 1/1/11	SIGNATURE		DATE
SIGNATURE		DATE	SIGNATURE		DATE

SECTION 2 (TO BE COMPLETED BY PAYEE OR FINANCIAL INSTITUTION)

GOVERNMENT AGENCY NAME USDA-NRCS	GOVERNMENT AGENCY ADDRESS 6013 Lakeside Blvd. Indianapolis, IN 46278
--	---

SECTION 3 (TO BE COMPLETED BY FINANCIAL INSTITUTION)

NAME AND ADDRESS OF FINANCIAL INSTITUTION PNC Bank 1234 Main Street Maintown, IN 98765				ROUTING NUMBER					CHECK DIGIT			
				1	2	3	4	-- 5	6	7	8	9
DEPOSITOR ACCOUNT TITLE Checking Account												
FINANCIAL INSTITUTION CERTIFICATION I confirm the identity of the above-named payee(s) and the account number and title. As representative of the above-named financial institution, I certify that the financial institution agrees to receive and deposit the payment identified above in accordance with 31 CFR Parts 240, 209, and 210.												
PRINT OR TYPE REPRESENTATIVE'S NAME				SIGNATURE OF REPRESENTATIVE				TELEPHONE NUMBER		DATE		

Financial institutions should refer to the GREEN BOOK for further instructions.

THE FINANCIAL INSTITUTION SHOULD MAIL THE COMPLETED FORM TO THE GOVERNMENT AGENCY IDENTIFIED ABOVE.



MARCH 2011

NRCS

Volunteer Time Tracking Portal V2.0

Volunteer Time Tracking Help Manual
Administrators and Coordinators

CONTENTS

	<u>Page</u>
1 Accessing the Volunteer Tracking System	2
2 Administration Page.....	3
3 Establishing New Administrators and New Volunteers	3
4 Create New Volunteer	4
5 Managing User Account Information	4
6 Entering and Verifying Time	5
7 Archive a Volunteer or Administrator	5
8 Create a New Volunteer Group	6
9 Edit an Existing Group	6
10 Add Group Members to a Reoccurring Group	7
11 Add Hours to a Group	7
12 Archiving a Group.....	8
13 Generate Reports	9

FIGURES

Figure 1: Portal Login Screen	2
Figure 2: Administration Screen	3
Figure 3: Create New User/Volunteer Screen	4
Figure 4: Group Time Sheet.....	7

Getting Started: A Guide for the New Volunteer Tracking System

You have been granted access to the new Volunteer Tracking System and the offices in your state have been assigned to you.

1 Accessing the Volunteer Tracking System

To access the Volunteer Tracking System, go to the tracking link site at:

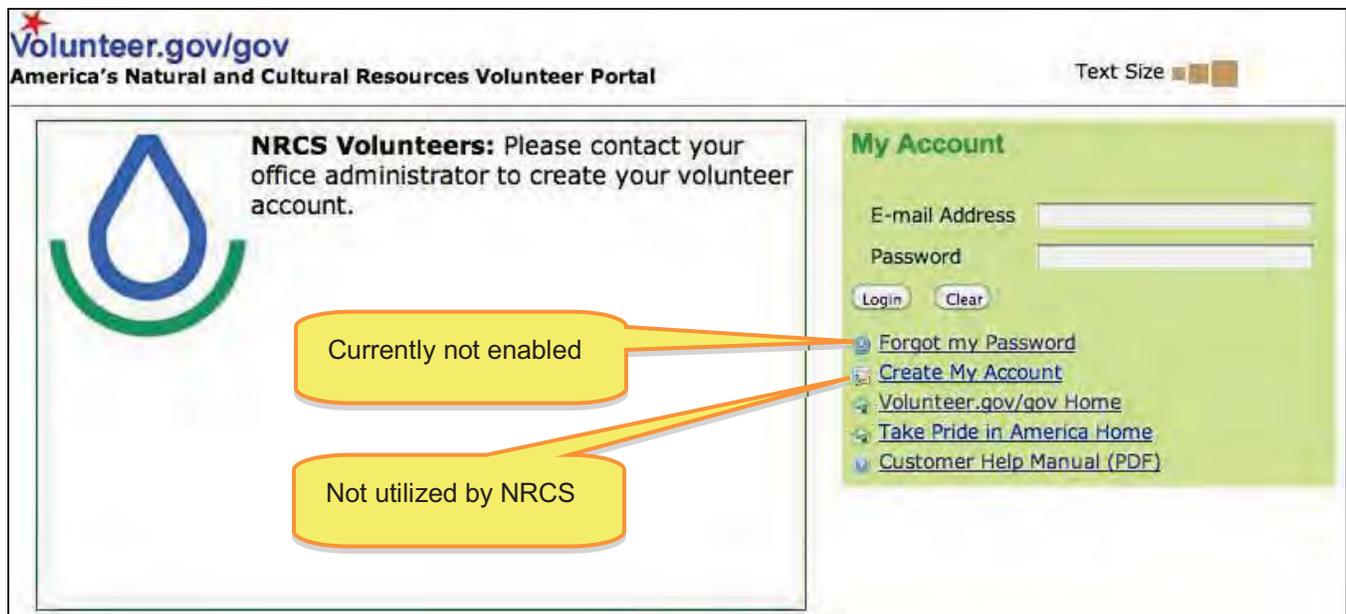
PORTAL LINK: <https://www.volunteer.gov/gov/VT/>

(This link can be found on My.NRCS under the Earth Team heading)

Your *User Name* is your government e-mail address and the *Password* is currently set at "password" (lower case). (See Figure #1 Login Screen)

NOTE: If you are unable to access the Volunteer Tracking System contact the National Earth Team Office.

Figure 1: Portal Login Screen



2 Administration Page

Once you have logged into the Volunteer Tracking System you will see the *Administration Page* with three green boxes. These boxes are your key menu areas to access sections of this portal. (See Figure #2: Administration Screen Note: Your actual administration screen may look slightly different depending on your user level):

1. Manage Users
 - 1.1 NRCS Groups
2. Generate Reports
 - 2.1 My Favorite Reports
3. Timesheets

Figure 2: Administration Screen



3 Establishing New Administrators and New Volunteers

The State Volunteer Coordinator will decide who receives Area or Office Administrative rights. Once an NRCS Employee is granted access, they will have the ability to establish and maintain Volunteer records.

The tracking system allows volunteers to enter their own hours and requires the administrator to verify the time.

Volunteer Coordinators/Administrators can create new volunteer and administrator accounts from the *Administration Page* by clicking the *Create New Volunteer* link and filling in the required information. Each required field is marked with a red asterisk *. Please refer to the next screen shot (Figure #3) and section 4 for instructions on creating a new user/Volunteer account.

Figure 3: Create New User/Volunteer Screen

Create New Volunteer

First Name *	Last Name *	Gender <input type="radio"/> Female <input type="radio"/> Male
Date of Birth <i>Not Used</i>	Phone	Email *
Address *	Address 2	City *
State <input type="text" value="Maryland"/> *	Zip Code *	Password *
Confirm Password *	User Name	User Level <input type="text" value="Volunteer"/> * <input type="text" value="NRCs"/> *
Completed Background Investigation <input type="radio"/> Yes <input type="radio"/> No	Office	

Office:
AK: ALASKA STATE OFFICE (104768)
AK: ANCHORAGE SERVICE CENTER (80026)
AK: BERING STRAITS RESOURCE CONSERVATION & DEVELOPMENT (106552)
AK: BETHEL SERVICE CENTER (106740)
AK: COPPER CENTER FIELD OFFICE (107007)
AK: COPPER VALLEY RC&D OFFICE (107008)
AK: CRAIG RESOURCE CONSERVATION & DEVELOPMENT (106738)
AK: DELTA JUNCTION SERVICE CENTER (80033)

Submit Reset

* = Required Note: User Name same as email address

4 Create New Volunteer

NOTE: You will need to select a user level from the drop down menu for each user (i.e. if you are creating a new volunteer user account, select the user level *Volunteer*.)

Once you type in the e-mail address for a new user, the information will be automatically transferred to the *User Name* field. If the user does not have an e-mail address you can create an account by using their first name period last name (i.e. *bonnie.allely*) and assign a password for the account.

All volunteers and administrators **must** be assigned to at least one office. To assign more than one office hold down the Control key, use your mouse and click on the office name. The offices will be highlighted in blue once they have been selected. If you have selected a wrong office, hold down the Control key and click the name of the office again and the blue highlight will disappear. If you want to select all offices, select the first office then hold down the Shift key and select the last office and it will highlight all offices between the first office you selected and the last one.

5 Managing User Account Information

Administrators can manage user account information for existing users including contact information, passwords, and user level access. To manage a user, select the desired name from the drop down menu on the *Administration Page* and click the *Manage* button. When searching for a specific volunteer/administrator on the “Administration Page”, right click on the name block, type the last name of the volunteer and it will automatically go to that name and select manage. The user details are displayed and can be updated or changed. As of 2011 the *User Name* can be changed by a National Administrator – if you make an error in inputting the User Name and you want this corrected, contact the National Earth Team Office.

NOTE: One of the key features of the *Manage Users* function is to reset a user's password. To reset a password, type the new password into the password field. The user can then go to the *Volunteer Tracking Portal* and click the *Forgot My Password* link to recover their new password. NOTE: As of 2011, the *Forgot My Password* link has been disabled for security purposes.

You can view or print volunteer work history for a specific time period from this page as well. When you are viewing a volunteer record you can scroll down to the bottom and you will see a yellow box titled "Generate Volunteer Work History". This allows you to see what dates the volunteer has worked and/or what timesheets you have already entered for a specific time frame.

6 Entering and Verifying Time

Administrators can enter and manage time for volunteers from the *Administration Page*.

1. Select the volunteer from the *Manage Existing Users* drop down menu
2. Click the *Manage* button
3. Scroll down to the calendar below the volunteer information screen
4. Click on a date and you will be navigated to the *Time Entry* screen

The weekly timesheet starts on Sunday and runs through Saturday. A *Volunteer Work Location* and *Activity Code* **must** be selected from the drop down menus. Tab over to the correct date and type in the hours. Click the *Save* button in the lower left corner once you have finished. The time entry process for administrators is identical.

If you need to enter more hours you may continue to select the date from the calendar and continue. If you need to edit the hours you input, click *Edit Timesheet*. Once you have finalized timesheets, click on *Administration Page* at the bottom or top of the page.

All timesheets must be verified. Once you have entered time and selected *Save*, you can verify the record by scrolling to the right and clicking *Verify*. Once an individual timesheet has been verified the only way to make a change to that weekly timesheet is to bring up the timesheet and go to the complete left and there click on the trashcan and delete the entire timesheet and then reenter it. You can make changes to timesheets before they are verified.

Timesheets that have not been verified will appear on the bottom half of the *Administration Page*. To verify timesheets from the *Administration Page*, select the volunteer name, scroll to the right and click *Verify*.

7 Archive a Volunteer or Administrator

From the *Administration Page* in the *Manage Users* box select the individual and select *Manage User*. In the lower left corner of the contact information there is a box that says *Archive User*, select *yes* or *no*. This gives you the ability to archive or un-archive a user at any time. Utilizing this function will have no impact on the reporting feature (i.e. if you archive a

user who has hours associated for the time period you selected, their time will be included on the report).

Each month any individuals who have been archived with zero hours will be automatically deleted from the system. This will only affect individual entries and not groups.

8 Create a New Volunteer Group

The Volunteer Tracking System is designed to allow NRCS users to manage volunteer groups. These groups consist of reoccurring and non-reoccurring (one-time volunteer groups). To access the *My Group Portfolio Page*, click on the *Manage Groups* link from the *Administration Page*.

The key functions of the *My Group Portfolio Page*:

1. Create New Groups
2. View Archived Groups
3. Edit Existing Groups
4. Add New Group Members
5. Add Group Timesheets

To create a new volunteer group, click *Manage Groups* from the *Manage Users* box on the *Administration Page*. Select *New Group* and you will be navigated to the *Create New Group Page*. Add the information specific to your group and click *Add Group*. You will be navigated back to the *My Group Portfolio Page* and the new group will be listed. At any time, you may click on the group's name to edit their information.

NOTE: When you edit group information, your edits will apply to all timesheets and group members associated with your group. For example, if you move a group from one office to another, all associated group members and timesheets will be automatically moved with your group.

9 Edit an Existing Group

At any time, you can edit an existing group. To edit a group from the *My Group Portfolio Page*, click on the name of your group in the groups table.

The *Edit Existing Group* screen includes all of the required information for your group. Additionally, from the *Edit Existing Group*, you can archive or re-activate a group by selecting the appropriate button. When completed, click *Edit Group* to save your changes.

10 Add Group Members to a Reoccurring Group

To add group members to an existing reoccurring group, from the *My Group Portfolio Page*, click on the *Timesheets/Group Members* link for your desired group. This will navigate you to the *Group Timesheet Page*. To add a new group member, fill in the information under the *Add New Member* section of the members table. Information includes: first name, last name, email address, and phone number. If you do not have the group member's email address and/or phone number, type *none*. When complete, click *Add Volunteer* to add your new group member/members.

NOTE: The group leader will need to be added as a group member in order to input time for that individual. One-time or non-reoccurring groups will not ask you for member names, but will ask for the number of members in the group along with total number of hours.

11 Add Hours to a Group

There are two ways to add time for individual group members. First, click on the calendar for the day you would like to add time. The date selected will appear next to all of the group members. Type in the hours for each member and select the *Activity/Date Worked* from the drop down menu. Verify that the date worked is correct and click *Add*. NOTE: As of 2011, the groups time sheet has been updated to allow you to add hours for all members at the same time by clicking the *Save All Time* (See Figure #4).

Figure 4: Group Time Sheet

Group Members/Hours Work Date: 03/17/2011			
Name	Hours	Activity/Date Worked	Total Hours
 Fischel, Pat	4	Accountability and Budget Performance Integration	0
 Fischel, Tom	3	Chesapeake Bay Initiative	0
 Stewart, Keith	2	Electronic Government	0
 Stewart, Gordon	1	Peoples Garden Initiative	0
<input type="button" value="Save All Time"/>			
Total Group Members: 4			0
Total Group Members with Hours This Work Date: 0			
Add New Group Member			
<input type="text"/>	First Name		
<input type="text"/>	Last Name		
<input type="text"/>	Email		
<input type="text"/>	Phone		
<input type="button" value="Add Volunteer"/>		<input type="button" value="Reset"/>	

New Save All Time button which allows you to save all members time with "one click"

You can also add time by modifying the date in the *Date Worked* area for each member. This may be useful when group members work on different days. You can change all time for each member and click the save button once, you do not have to hit the Save All Time button.

NOTE: Group time can only be input by an administrator and does not have to be verified.

As you enter time, a running total of time for your group is shown below your group members. Additionally, your members' time is also shown to the right of the member's row.

If you wish to get more information about an individual member's time, click on the member's name to see their timesheets.

You can edit a group member's timesheet at any time. To edit a timesheet, find the timesheet you wish to edit and enter the new hours for the member. If you need to remove hours for a member on a given date, find the members timesheet and enter a 0 (zero) for the selected member and date.

12 Archiving a Group

Just as you can archive an individual volunteer, you also have the ability to archive an entire group or specific group members. Once archived, the group or group member will no longer show up as active.

To archive or reactive a group, click on the group name and select either *Yes* or *No* to Archive.

13 Generate Reports

The Volunteer Tracking System provides real-time statistical data.

From the Administration Page you can generate the following reports by the range of dates that you input:

1. National Report by National Offices
 - # of Volunteers
 - # of Hours
 - # of Offices Actively Using Volunteers
 - % of Offices Using Volunteers
 - # of National Offices in the State
2. National Report by State
 - # of Volunteers
 - # of Hours
 - # of Offices Actively Using Volunteers
 - % of Offices Using Volunteers
 - # of Offices in the State
3. National Report By Activity Code
 - Lists Activity
 - # of Volunteers Nationally Performing This Activity
 - % of Volunteer Hours in Each Activity
 - Total Hours in Each Activity
4. National Report by Regions (States)
 - # of Volunteers by Region
 - # of Hours by Region
 - # of Offices Actively Using Volunteers by Region
 - # of Offices in the State by Region
 - % of Offices Using Volunteers by Region
5. National Report by Regions (Activity Codes)
 - Same Report as #3 – you select the Region
6. NRCS State Report By Activity Code
 - Same Report as #3 but you select the State
7. Custom Report by Area/Office/Volunteer
 - This is a build your own report from the offices that you are an administrator for. It will give you a report that lists:
 - OIP Address
 - Office Name
 - Volunteer Name
 - # of Hours

Group Name
of Members in Group
of Group Hours

8. Custom Report by Area/Office/Activity

This is a build your own report from the offices that you are an administrator for. It will give you a report that lists:

OIP Address
Office Name
Individual Activity
Individual Hours
Group Activity
Group Hours

9. Active Volunteers (Addresses and Offices)

First Name
Last Name
Street Address
City
State
Zip Code
Phone
Office Name

All custom reports can be saved as a favorite and will be updated as additional information is input into the database as the reports are real-time statistics.

All reports can be downloaded into an Excel spreadsheet for your use in developing graphs and other reports as needed.