

For: State and County Offices

Mandatory FSA Computer Security Awareness Training

Approved by: State Executive Director



1 Overview

A Background

The Computer Security Act of 1987 Public Law 100-235) and the Office of Management and Budget's Circular A-130 (Management of Federal Resources), Appendix II Security of Federal Automated Information Resources) require mandatory periodic Security Awareness training and accepted computer security practice training for FSA employees (excluding COC Members and Advisors).

It is the responsibility of supervisors to ensure that all employees they supervise are trained in Security Awareness. It is the responsibility of every employee to ensure they understand and execute security.

The security training materials provided in this notice are also available at the following web address: <http://intranet.fsa.usda.gov/fsatraining>

B Purpose

The purposes of this notice are to:

- Provide the following enclosures to be read/studied by all FSA employees:
 - February 13, 2003 memorandum from Francis R. Shehan. See Exhibit 1.
 - Computer Security Awareness Training Information. See Exhibit 2.
 - Certification of Completion Memo Format in Exhibit 3.
 - Good Computer Security Practices. See Exhibit 4.

Disposal Date

July 1, 2003

Distribution

County Offices

1 Overview, Continued

B Purpose, Continued

- Inform all FSA employees of the mandatory requirements to complete the enclosed Security Awareness training and certify completion by May 30.
- Provide guidance for employees to certify completion of training through ICAMS in lie of manually certifying. See Exhibit 5. **NOTE:** Temporary employees will not use the ICAMS method of certifying. They must send the Certification of Completion (Exhibit 3) to the STO Adm Section.
- Provide guidance for supervisors to certify through ICAMS that they have verified employee completion of the required Security Awareness training. See Exhibit 6.

C Contact

For questions regarding this notice, please contact Jan Courtright at the State Office.

D Deadline

By May 30:

- All employees shall complete and certify to completion of the enclosed mandatory Security Awareness Training.
- All supervisors shall verify that all employees they supervise have completed and certified to completion of this training.

E Who is to be Trained

All GS and CO employees (excluding COC Member and Advisors) shall receive the enclosed training.

2 Action

A Employees Certification

After the enclosed Security Awareness training has been completed, the employee shall register for ICAMS catalog course number 020097.

Note: The employee's ICAMS registration is considered to be the employee's certification that he/she has completed the training. The manual certification of completion for training in Exhibit 3 shall only be used by temporary employees.

Guidance is provided in Exhibit 5 for employees to register/certify through ICAMS.

OK Notice PM-1374

2 Action, Continued

B Supervisors Verification

After employees certify their completion of the enclosed training by registering for ICAMS catalog course 020097, the request flows to their supervisor's worklist and supervisors will receive an e-mail to notify them they have a related worklist item. Supervisor shall approve the training request after they verify training was completed by the applicable employee.

Using this method, there is no need for a hard copy manual certification.

Guidance is provided in Exhibit 6 for supervisors to approve/verify Security Awareness training for their employees through ICAMS.



United States
Department of
Agriculture

February 13, 2003

Farm and Foreign
Agricultural
Service

Farm Service
Agency

1400 Independence
Ave, SW
Stop 0580
Washington, DC
20250-0580

TO: Farm Service Agency and Foreign Agricultural Service Employees,
Contractors, Subcontractors, Grantees, and Co-operators

FROM: Francis R. Shehan
Director
Information Technology Services Division

SUBJECT: Mandatory Farm and Foreign Agricultural Service (FFAS) Computer
Security Awareness Training--REVISED

The FFAS Information Systems Security Program is providing computer security awareness information for you to read and use to help protect FFAS resources from unauthorized access, modification, use, and disclosure. All FFAS employees, contractors, subcontractors, grantees, and cooperators are required to complete their yearly **mandatory** computer security awareness training by reading this information and then mailing a signed certification form that they have done so by **May 30, 2003**.

Computer security is everyone's responsibility. You are the key.

REVISIONS: The deadline has been extended from December 20, 2002. The revised directions explain that all Farm Service Agency (FSA) State office and County Office employees, both Federal and non-Federal (except state and county committee members), need to take this training. In addition, minor changes were made to the exhibit forms. However, please note that if one has already completed the training and mailed the certification form, then no further actions are needed.

The Computer Security Act of 1987 (Public Law 100-235) and the Office of Management and Budget's Circular A-130 (Management of Federal Resources), Appendix III (Security of Federal Automated Information Resources), require mandatory periodic training in computer security awareness and accepted computer security practice of all employees and contractors who are involved in the management, use, or operation of a Federal computer system within or under the supervision of the Federal agency. USDA also requires training for employees and contractors who use output from computer systems.

04-09-03

Page 1

FSA and FAS Employees, Contractors, Grantees, and Co-operators **2**

Therefore, each FFAS employee and contractor shall complete the following actions by **May 30, 2003**.

- Receive two hours of official time to read the following electronic files:
 - ◆ This letter (ltrsec02.doc or ltrsec02.wpd)
 - ◆ FFAS Computer Security Awareness Training Information, (sectrn02.doc or sectrn02.wpd).
- Complete the appropriate certification process, either by requesting Computer Security Training 2002 or training course #020097 in the I-CAMS web (for those offices that have adopted the I-CAMS web) or by completing and submitting Exhibit 1 (1-FSA or 1-FAS), 2 or 3.

Note: Managers and supervisors are responsible for ensuring that their employees and contractors understand their security responsibilities and policies and are in compliance with this memorandum. They may want to coordinate and collect their staff's forms for submission. Managers and supervisors are also responsible for ensuring that new employees and contractors shall complete the training within 60 days of being hired.

Use the following information to determine which certification form (Certification of Completion) to use and who to contact for more information.

- FSA offices in the Washington, DC area should complete **Exhibit 1-FSA by May 30, 2003** and send it to:

USDA/FSA/HRD/TDB STOP 0574
ATTN: Tracey Foster
1400 Independence Avenue, SW
Washington, DC 20250-0574

Telephone number: (202) 418-9051

FAX number: (202) 418-9131

- All FAS Offices should complete **Exhibit 1-FAS by May 30, 2003** and send it to:

USDA/FSA/HRD/TDB STOP 0574
ATTN: Marie Hubbard
1400 Independence Avenue, SW
Washington, DC 20250-0574

Telephone number: (202) 418-9047

FAX number: (202) 418-9131

FSA and FAS Employees, Contractors, Grantees, and Co-operators **3**

- FSA Aerial Photography Field Office and the FSA Kansas City Office should complete **Exhibit 2 by May 30, 2003** and send it to:

USDA/FSA/KCAO/PD/EDB STOP 8398
 ATTN: Jewel Roberts
 6501 Beacon Drive
 Kansas City, MO 64133-4676

Telephone number: (816) 926-6263

FAX number: (816) 926-1825

- FSA State Offices and County Offices employees (both Federal and non-Federal, except state and county committee members) should complete the following **by May 30, 2003**:
 - ◆ Request Security Training Course 2002 or training course #020097 per I-CAMS web.
 - ◆ If not using I-CAMS web, complete **Exhibit 3** and submit to your State Training Officer.

This section identifies the Information Systems Security Program Officials of the FFAS Washington, DC and Kansas City, MO security offices. If you have information systems security questions or problems, please contact:

FFAS INFORMATION SYSTEMS SECURITY PROGRAM OFFICIALS**FSA and FAS Metropolitan Washington, DC Offices and FAS Field Offices**

USDA-FSA-ITSD-PPB-ADPTSSS STOP 0584
 1400 Independence Avenue, SW
 Washington, DC 20250-0584

Brian J. Davies, FFAS Information Systems Security Program Manager (202) 720-2419
 FAX: (202) 720-7134

Seabelle J. Ball, Information Systems Security Officer	(202) 205-7399
Patricia B. Gray, Information Systems Security Officer	(202) 720-2599
Eric M. Miller, Information Systems Security Officer	(202) 720-0146
Sue Weis, Information Systems Security Officer	(202) 690-4639
Roger W. Scaife, Deputy Information Systems Security Officer	(202) 720-9152

FSA and FAS Employees, Contractors, Grantees, and Co-operators **4****FSA Kansas City Office and FSA Field Offices**

USDA-FSA-KCITSTO-ISSPS STOP 9198

6501 Beacon Drive

Kansas City, MO 64133-4676

Anthony J. Capo, FSA KC Office Information Systems Security Program Manager

(816) 926-1485

FAX: (816) 926-6090

**FSA KC Office Information Systems Security Help Desk
(Staffed by three Contract Employees)****(816) 926-6537****FAX: (816) 926-6090**

Linda N. Allen, Information Systems Security Officer	(816) 823-1070
Janell S. Duke, Information Systems Security Officer	(816) 926-1641
Noah W. Edmeier, Information Systems Security Officer	(816) 823-1995
Mindy J. Gehrt, Information Systems Security Officer	(816) 926-7323
Jerry D. Hall, Information Systems Security Officer	(816) 926-6290
Kurt R. Hoffman, Information Systems Security Officer	(816) 926-3709
Marcia A. McCarty, Information Systems Security Officer	(816) 926-3024
Gail S. Phillips, Information Systems Security Officer	(816) 823-1818
Andrew K. Solomon, Information Systems Security Officer	(816) 926-6910

Attachments

cc: Director/ITSD/Room 5768-S
ITSD READER FILE
Lori Beutel/ITSD/PPB
Brian J. Davies/ITSD/PPB/ADPTSSS
PPB READER FILE

FSA/ITSD/PPB/BDavies/720-2419/sm/02-12-2003/s:memo\sonja\LTRSEC02-new.doc

**FARM AND FOREIGN AGRICULTURAL SERVICE (FFAS)
INFORMATION SYSTEMS SECURITY PROGRAM**

**COMPUTER SECURITY AWARENESS
TRAINING INFORMATION**



**U.S. DEPARTMENT OF AGRICULTURE
FARM SERVICE AGENCY (FSA)
FOREIGN AGRICULTURAL SERVICE (FAS)
RISK MANAGEMENT AGENCY (RMA)**

SEPTEMBER 2002
(Minor Updates--February 2003)

**Farm and Foreign Agricultural Service (FFAS)
Computer Security Awareness Training Information**

**All Employees and Contractors
Farm Service Agency
Foreign Agricultural Service
Risk Management Agency**

TABLE OF CONTENTS

<u>Subject</u>	<u>Page</u>
Why Computer Security Awareness Training? It's the Law!.....	1
Computer Security Roles and Responsibilities-FSA Notice IRM-307.....	1
Security Violations.....	2
Key Computer Security Terms	3
What is a Computer Security Program?	3
How Much Security Is Enough?	3
Sensitive Information.....	4
Protecting Classified Information-FSA Notice IRM-313.....	4
Limited Personal Use Policy.....	4
Internet Use Guidelines-FSA Notice IRM-306	5
E-Mail General Policy-FSA Notice IRM-306	5
Unacceptable Uses of E-Mail	5
Internet E-Mail with Attachments	6
Computer Software Piracy and the Copyright Act	6
Games and Unauthorized Software	6
"Peer-to-Peer" Software Installation and Use Specifically Prohibited.....	7
Good Computer Security Practices.....	8
Computer Security Threats	9
Applying Some Common Sense	10
"Social Engineering"	10
Password Guidance.....	11
Security Reminder - Protecting Laptop Computers.....	12
Computer Virus Detected - Who to Call.....	13
For More Security Information: Visit a FFAS Security Web Site.....	14
Information Systems Security Summary	14
Thank You!	14
Appendix A FFAS Information Systems Security Program Officials	15
Appendix B FFAS Internet and Electronic Mail (E-Mail) Policy Overview.....	16
Appendix C Computer Security Federal Laws, Executive Orders, Presidential Decision Directives, Regulations (Government-wide, USDA, and Department of State), Agency Policies, and Guidance	23

**FARM AND FOREIGN AGRICULTURAL SERVICE (FFAS)
COMPUTER SECURITY AWARENESS TRAINING INFORMATION**

WHY COMPUTER SECURITY AWARENESS TRAINING? IT'S THE LAW!

The **Computer Security Act of 1987**, Public Law (Pub. L.) 100-235 and the Office of Management and Budget's (OMB) **Circular A-130**, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources, require mandate periodic training in computer security awareness and accepted computer security practice of all employees and contractors who are involved in the management, use, or operation of a Federal computer system within or under the supervision of the Federal agency.

USDA Departmental Regulation 3140-1, USDA Information Systems Security Policy, states that: "All USDA agencies must make security awareness and training mandatory for all employees that use, operate, supervise, or manage computer systems or use output from computer systems. Each USDA employee that uses computers or output from computers must be:

- a Provided awareness of their security responsibilities;
- b Provided periodic security training (minimum once a year) in how to fulfil the responsibilities of security; and
- c Informed of requirements as stated in OMB Circular A-130 relating to awareness and training."

It also requires that Agency Information Systems Security Program Managers: "Develop and conduct computer security awareness training for security personnel, employees, and contractors to meet the training program requirements of the Computer Security Act of 1987."

The three policies below (which will be updated and reissued) apply to FSA, FAS, and RMA:

- ! FSA Notice IRM-306, FFAS Internet and Electronic Mail (E-Mail) Policy.
- ! FSA Notice IRM-307, Information Systems Security Program.
- ! FSA Notice IRM-313, Protecting Classified Information.

For a list of Federal laws, executive orders, regulations, and agency polices that apply to computer security in FFAS, please refer to **Appendix C**.

COMPUTER SECURITY ROLES AND RESPONSIBILITIES-FSA NOTICE IRM-307

One fundamental issue that arises in discussions of computer security is: "Whose responsibility is it?" A simple answer is: **Computer Security is Your Responsibility**.

FSA Notice IRM-307, Information Systems Security Program, contains policy and procedures for implementing the FFAS Information Systems Security Program. It defines authorities, responsibilities, and security controls. It provides security measures and safeguards to protect information resources from unauthorized access, use, modification, and disclosure. The notice states the importance and value of computer and information resources, and the need to preserve and protect their integrity, confidentiality, and availability.

All employees and contractors are required to protect Government resources from accidental or deliberate unauthorized access, use, modification, or disclosure by employing adequate security measures through cost-effective technical and management controls. All employees and contractors are personally accountable for Government resources entrusted to them and protecting sensitive program data.

All FFAS computers, data, and information resources are for official use and limited personal use (see page 4 and **Appendix B**, FFAS Internet and Electronic Mail (E-Mail) Policy Overview).

Employees' and contractors' responsibilities include:

- ! Request appropriate access authorization from the supervisor and fill out any necessary request forms.
- ! Ensure that user identification codes, "userids" (unless they are the employees' names), and passwords are held in strict confidence and properly safeguarded from unauthorized access, use, and disclosure.
- ! Understand and comply with all security requirements in Federal laws and FFAS and USDA policies.
- ! Refrain from exploiting any hardware, software, communications, or automated information system weakness, such as intentionally modifying, destroying, reading, or transferring data and information in an unauthorized manner.
- ! Provide correct userids and use only authorized computer systems, data, and information resources.
- ! Secure and log off (or password protect your computer session) your computer when leaving the office area. Secure and log off from any computer when processing is done. Always log off at the end of the workday.
- ! Refrain from introducing any unauthorized or unscanned software, data, hardware, or telecommunication devices or modifying any configuration without proper approval from the Chief Information Officer (CIO) for the agency. Please note that this also prohibits interfacing your Personal computer (PC) with a Personal Digital Assistant (PDA) unless this is done in accordance with agency policy and procedures (which are currently under development).

SECURITY VIOLATIONS

- ! Management has the authority to examine and monitor Government resources entrusted to you including E-Mail and Internet messages to ensure compliance with appropriate policies.
- ! Any person who willfully violates Federal laws or FFAS and USDA policies is subject to disciplinary action, including suspension or dismissal.
- ! Report any observed or suspected computer security incident, breach, or violation to your immediate supervisor and local Information Systems Security Officer for appropriate investigation.

KEY COMPUTER SECURITY TERMS

Confidentiality is the requirement that private or sensitive information not be disclosed to unauthorized individuals. **Integrity** in the computer security field has two aspects: data integrity and system integrity. **Data integrity** is the requirement that information and programs are changed only in a specified and authorized manner. Protection is required from unauthorized, unanticipated, or unintentional data modification. **System integrity** is the requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. **Availability** is the requirement intended to assure that systems work promptly and service is not denied to authorized users.

Another security goal is **Accountability**, the requirement for actions by a user to be traced uniquely to that user. It includes **Non-repudiation**, ensuring someone who receives data (such as an E-mail message) can be sure from whom the message came from (proof of origin) and someone who sends data can be sure that the message was received (proof of delivery). System accountability depends upon the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. This is especially important in Electronic Commerce. **Authentication**, the verification of a user's identity before allowing the user access to a system, is also important.

Assurance is the grounds for confidence that the other four security goals (integrity, confidentiality, availability, and accountability) have been adequately met by a specific implementation.

If you are interested in more information on computer security terms and a beginner's guide to computer security, please access the following web site sponsored by the National Cyber Security Alliance (a hyperlink to this site is in this document, so you should be able to click on the link to visit it):

http://www.staysafeonline.info/appendix_b.adp

Note that there can sometimes be problems with hyperlinks, so if the hyperlink does not work, please copy the site's Internet address and paste it directly into your Internet browser (Netscape or Internet Explorer).

WHAT IS A COMPUTER SECURITY PROGRAM?

The primary goal of the FFAS Information Systems Security Program is to protect FFAS computing and information resources from inadvertent and unauthorized:

- ! Disclosure,
- ! Alteration or destruction, and
- ! Use.

This is achieved by ensuring the confidentiality, integrity and availability of FFAS Information Technology resources.

Information Security = Confidentiality, Integrity, and Availability (remember "CIA")

HOW MUCH SECURITY IS ENOUGH?

No matter how many controls or safeguards we use, we can never achieve total security. We can, however, decrease the risk in proportion to the strength of the protective measures. The degree of protection is based on the value of the information; in other words, how serious would be the consequences if a certain type of information were to be wrongfully changed, disclosed, delayed, or destroyed?

SENSITIVE INFORMATION

Many people think that sensitive information is only information that requires protection from unauthorized disclosure. However, the **Computer Security Act of 1987** provides a much broader definition of the term sensitive information as follows:

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act of 1974), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

PROTECTING CLASSIFIED INFORMATION-FSA NOTICE IRM-313

This notice reminds all FSA, FAS, and RMA employees and contractors with access to classified information of their duty and responsibility to protect classified information against unauthorized disclosure in the interest of national security. Using FSA, FAS, and RMA unclassified Local Area Networks (LAN's) to store or process classified information is absolutely prohibited.

PCs used for storing or processing classified information shall:

- ! Have approved security measures, such as removable hard disks which can be locked up.
- ! Have secure telecommunications (if applicable).
- ! **NOT** be connected to an unclassified network.

Users are also reminded that unclassified electronic mail (E-mail) systems and the Internet are not secure and shall **NOT** be used to transmit classified information.

LIMITED PERSONAL USE POLICY

FFAS policy follows USDA Departmental Regulation (DR) 3300-1 in that it authorizes the **limited personal use** of the Internet, with supervisory approval, and of E-mail "in the workplace on an occasional basis provided that the use involves minimal expense to the Government and does not interfere with official business. Occasional personal use of telecommunications resources shall take place during the employees' personal time. This policy follows the CIO Council's model for guidance on limited personal use." For more information, please see FSA Notice IRM-306, FFAS E-Mail and Internet Usage, or **Appendix B** of this document, FFAS Internet and Electronic Mail (E-Mail) Policy Overview.

Please note that DR 3300-1 states that: "Misuse or inappropriate personal use of government office equipment includes: Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network. "Push" technology on the Internet and other continuous data streams would also degrade the performance of the entire network and be an inappropriate use." Therefore, users should also not consume USDA Internet bandwidth by playing music or videos through the USDA Internet connection for their personal use. Also, users should not use Government resources which may be needed for official business for their personal use. Therefore, users should not store their personal data files, especially large video or music files (please also see the section on copyright protection given later in this document) on network disk drives, since this uses disk space that could be used instead for official purposes.

INTERNET USE GUIDELINES-FSA NOTICE IRM-306

Specifically, the Internet shall **NOT** be used:

- ! For personal gain or profit. It cannot be used to earn outside income or otherwise to obtain financial gain. For example: stock trading or support of outside employment or business activity.
- ! For uses which reflect adversely on USDA or you (such as pornography, gambling, and games)
- ! To misrepresent yourself as someone else.
- ! For solicitation of Government employees.
- ! To provide information about or lists of USDA employees to others without authorization.
- ! When it interferes with your job or the jobs of other employees.
- ! When it interferes with the operation of the Internet gateways.

E-MAIL GENERAL POLICY-FSA NOTICE IRM-306

USDA DR 3300-1, Appendix F, "Electronic Messaging and Voice Mail," states the following:

- ! "Electronic mail shall be used for the conduct of official business or limited personal use."
- ! "Electronic mail messages containing discriminatory language or remarks that may constitute sexual harassment are prohibited."

UNACCEPTABLE USES OF E-MAIL

E-Mail shall **NOT** be used for the transmission of

- ! Sexually explicit information (including pornography).
- ! Racially or ethnically insulting or religiously demeaning information.
- ! Any type of personal solicitation.
- ! Chain letters or other unauthorized mass mailings.
- ! Outside business activities.
- ! National security information or classified material (except on an approved classified network).

Information exempted from disclosure under Freedom of Information Act (5 U.S.C. 552) and information protected by the Privacy Act (Pub. L. 93-579, 5 U.S.C. 552) **shall not** be transmitted over the Internet and E-mail systems unless encrypted. Other sensitive information **shall not** be sent unencrypted over an unprotected (uncertified or unaccredited) E-mail system.

INTERNET E-MAIL WITH ATTACHMENTS

The Internet is a valuable tool for exchanging information. However, it is not secure, and the potential for receiving an attachment containing a computer virus is significant. Internet E-mail attachments must be scanned for viruses before opening and before saving to the hard drive or another storage device. Employees are responsible for ensuring each attachment is properly scanned. Usually systems are configured to scan for viruses automatically. Users must not try to remove or bypass anti-virus programs installed on the system.

COMPUTER SOFTWARE PIRACY AND THE COPYRIGHT ACT

Executive Order 13103, Computer Software Piracy, issued on September 30, 1998 states that: "The United States Government is the world's largest purchaser of computer-related services and equipment, purchasing more than \$20 billion annually. At a time when a critical component in discussions with our international trading partners concerns their efforts to combat piracy of computer software and other intellectual property, it is incumbent on the United States to ensure that its own practices as a purchaser and user of computer software are beyond reproach." The Executive Order establishes the following policy: "It shall be the policy of the United States Government that each executive agency shall work diligently to prevent and combat computer software piracy in order to give effect to copyrights associated with computer software by observing the relevant provisions of international agreements in effect in the United States, including applicable provisions of the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights, the Berne Convention for the Protection of Literary and Artistic Works, and relevant provisions of Federal law, including the Copyright Act."

All USDA employees and supervisors will protect the Government's interests as they perform their duties. This includes assuring that commercial software acquired by the Government is used only in accordance with licensing agreements. Likewise, they are to assure that any proprietary software is properly licensed before being installed on USDA equipment. This guidance does not apply to software developed by or for a Federal agency since no restrictions apply to its use or distribution within the Federal Government.

GAMES AND UNAUTHORIZED SOFTWARE

Installing and using software that is for personal use and/or private gain on a Government microcomputer or LAN is strictly prohibited. Even though limited personal use of Government equipment is now allowed, users are not allowed to install personal software (such as games), since it causes a configuration change to the equipment and may cause system configuration and system resource problems.

Examples of unauthorized software include:

- ! Income Tax Preparation Packages,
- ! Personal Checkbook Software,
- ! Private Mortgage Amortization Software, and
- ! Private Business Packages.

Installing, copying, displaying, demonstrating, or using sexually explicit material such as nude calendars or pornography is strictly prohibited. Examples include:

- ! Sexually Explicit Documents, and
- ! Sexually Explicit Graphics.

“PEER-TO-PEER” SOFTWARE INSTALLATION AND USE SPECIFICALLY PROHIBITED

Installing “peer-to-peer” file sharing programs (Napster and its successors, such as Gnutella, LimeWire, Swapnut, KaZaA, Morpheus, and other similar programs) or using them to download, upload, or swap files is prohibited on USDA computer systems. These programs not only encourage copyright violations, but they also cause security vulnerabilities in networks when they are installed. USDA’s Office of Cyber Security (OCS) is monitoring our networks for these types of activities and will detect them. They do not monitor individuals, but events. However, if they find illegal activity or activity that is against regulations, they can trace it back to a user.

On September 26, 2001, OCS sent out an E-Mail to security managers at all USDA agencies documenting the threats of peer-to-peer software and specifically banning its installation and use on USDA systems. Recently, they have noticed an increase in the attempts by some USDA employees and contractors to circumvent this prohibition. The use of peer-to-peer software not only violates policy, but in many instances, breaks the law by violating the Copyright Act. OCS has asked us to please remind all of our employees and contractors that USDA is in compliance with Executive Order 13103 and the violator is personally responsible for all costs incurred by violations of the Copyright Act. Installation and use of peer-to-peer software cannot be justified as being in compliance with the Federal CIO Council's Limited Personal Use Policy.

OCS has also asked us to share an article with our employees and contractors from the August 28, 2002 Denver Post: Downloading that new Britney Spears hit from the Net may come at a cost that includes divulging personal bank account information, credit card numbers and even company secrets. Millions of people, following the trend first set by Napster, use file-sharing websites not only to copy and download free music, but also find pictures, video clips, pirated software and documents from millions of others who open their computers to a virtual network. These so-called peer-to-peer websites allow people to download free files - primarily songs - stored on the computers of millions of other file-sharing users. What people do not understand is the risk involved in peer-to-peer transfers. If people rush through installation of the software, they can inadvertently open their entire hard drive to the world! File sharing carries a great inherent security risk.

**FARM AND FOREIGN AGRICULTURAL SERVICE (FFAS)
INFORMATION SYSTEMS SECURITY PROGRAM**

September 2002

TO: Farm Service Agency (FSA), Foreign Agricultural Service (FAS),
and Risk Management Agency (RMA) Employees and Contractors

GOOD COMPUTER SECURITY PRACTICES

Always Protect FFAS Information Resources - All classified, sensitive, private, and mission-critical information, data, systems, and applications require protection from unauthorized access, use, disclosure, alteration, and loss.

Know Our Policies - Read USDA, FFAS, FSA, FAS, and RMA directives, including FFAS Information Systems Security Program policies. FSA users must also follow applicable policies issued by the Service Center Modernization Initiative (SCMI) Information Technology Working Group (ITWG) approved by FSA.

Protect Your Work Area - Recognize, politely challenge, and assist people who **DO NOT** belong in the work area.

Prevent Unauthorized Access - Computer resources and equipment, especially personal computers and servers, should not be exposed to unauthorized access.

Protect Passwords - Use only passwords that are not easily guessed or in the dictionary, change them frequently, and **DO NOT** share your password with anyone.

Protect Your Files - Establish and periodically review access privileges for each file.

Protect Your Computer - Always logoff or password protects your screen before leaving your computer system unattended. Always safeguard software and removable media such as diskettes.

Protect Against Computer Viruses - Never load unauthorized or personal software on your computer system. Report viruses immediately to your supervisor and the appropriate Help Desk for corrective action. Before loading data from any media (diskette, Internet, etc.), always check it for viruses.

Protect Against Disaster - Always have backup program, equipment, and databases ready to go.

Protect Classified and Sensitive Data and Information - Read USDA, FFAS, FSA, FAS, RMA, ITWG and Department of State directives, policies, handbooks, and manuals. FAS' classified information will be handled in accordance with the USDA, FFAS, FAS, and the Department of State regulations.

Report Violations - Document any computer and communications misuse, abuse, security incident or breach. Report it immediately to your supervisor and your Information Systems Security Officer.

DO YOU HAVE A COMPUTER SECURITY QUESTION?

Please contact your Information Systems Security Officer at:

(FSA) Security Office at Kansas City, MO

(816) 926-6537, (816) 823-1070, (816) 926-1641, (816) 823-1995, (816) 926-7323, (816) 926-6290,
(816) 926-3709, (816) 926-3024, (816) 823-1818, (816) 926-6910, or (816) 926-1485

(RMA) Security Office at Kansas City, MO

(816) 926-7320, (816) 926-1341 or (816) 926-2730

Security Office at Headquarters in Washington, DC

(202) 720-0146, (202) 690-4639, (202) 205-7399, (202) 720-2599, (202) 720-9152, or (202) 720-2419

COMPUTER SECURITY THREATS

- ! **Denial-of-service (DoS)**-Incident in which a user or organization is deprived of the services of a resource they would normally have. Malicious attackers can shut down Web sites.
- ! **Dictionary Attack**-Sequentially trying common passwords or words from a dictionary to discover a user's password. This works best if the attacker can download the entire encrypted password file, and test passwords against it off-line by using the system's known password encryption method.
- ! **Distributed Denial of Service (DDoS)**-Attacks utilizing compromised ("zombie") computers to launch coordinated DoS attacks to simultaneously flood sites with more data than they can handle.
- ! **Employee Sabotage**-Destruction or malicious data alteration by an employee.
- ! **Fraud and Theft**-by both employees and outsiders.
- ! **Hacker (Cracker)**-Unauthorized user who breaks into computers for various purposes. Anyone who attempts to gain access or performs an operation that has not been granted access to do so.
- ! **Human Errors and Omissions**-User/operator error; inadvertent alteration, manipulation, or destruction of programs, data files, or hardware.
- ! **Industrial Espionage**-Gathering, transmitting, or losing information with respect to trade secrets with intent or reason to believe that the information is to be used to injure a specific company or the Government or to the advantage of a foreign nation or foreign nation's industry.
- ! **Loss of Physical and Infrastructure Support**-caused by changes in the physical environment-fire damage, water damage, power loss, civil disorder, and vandalism.
- ! **Mail Bomb**-A huge number of E-mail messages sent to one destination. Mail bombs are sent to antagonize their recipients and/or to cause them problems by filling up their disks and overloading the system.
- ! **Malfunction**-An equipment malfunction is hardware which operates in abnormal, unintended mode. A software malfunction is software behavior which is in conflict with intended behavior.
- ! **Masquerade**-Accessing a computer by pretending to have an authorized user's identity.
- ! **"Phone Phreak" ("phreak")**-A type of hacker who has a specific interest in the phone system and the systems that support its operations. A talented phreak is a threat to not only the telephone system, but to the computer networks it supports.
- ! **Scavenging (Dumpster Diving and Browsing)**-Accessing discarded trash to obtain passwords and other data. Usually automated scanning of large quantities of unprotected data from discarded or on-line media to obtain clues as to how to achieve access.
- ! **Snooping and Eavesdropping**-Electronic monitoring of networks to uncover passwords or other data. Direct visual observation of monitor display to obtain access.
- ! **Spoofing**-Getting a computer on a network to pretend to have the identity of another computer, usually one with special access privileges, to obtain access to other computers on the network.
- ! **War Dialing**-An attack in which an intruder dials all the numbers in an exchange to find modems.

Malicious Software:

- # **Trojan Horse**-A useful or apparently useful program containing hidden code that, when invoked, performs some unwanted function, such as the unauthorized collection, falsification, or destruction of information.
- # **Virus**-Self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. A computer virus infects other programs by modifying them to include a copy of itself. Unlike a worm, a virus cannot infect other computers without assistance, for example, when users share programs with their friends. Some viruses are relatively harmless, but others do irreversible damage such as deleting all user files or erasing the hard drive.
- # **Worm**-A self-replicating program that is self-contained and does not require a host program. It is designed to propagate through a network rather than just a single computer. A worm exploits flaws in operating systems or inadequate system configurations. Release of a worm usually results in brief, but spectacular, outbreaks that can shut down entire networks.
- # **Logic Bomb**-A virus or worm designed to activate under certain conditions.
- # **Time Bomb**-A virus or worm designed to activate at a certain date or time.

APPLYING SOME COMMON SENSE

Sophisticated security systems can fail if common sense is not used. Examples:

- ! Expensive lock on the computer room door but the door is propped open.
- ! User identification and password not secured (taped to monitor).
- ! Use of an obvious password (examples: the person's name or the person's pet's name).
- ! References not checked before hiring people in sensitive positions.
- ! Sensitive data and information on diskettes and printed reports left out in the open for anyone to view, copy, or use.

"SOCIAL ENGINEERING"

Beware of "**social engineering**," a technique used by hackers to trick people into revealing passwords or other sensitive system information. This technique is also called "people hacking" since it relies on obtaining information directly from people rather than hacking into a computer system by exploiting a technical flaw in the software or operating system, or trying to guess a user's password. Social engineering is often done by a hacker calling someone and asking for the user's computer userid and password or just the user's password. The hacker may also ask a user to reset his/her password to a password supplied by the hacker, or to change the password and tell the caller (the hacker) the new password. The person calling may pretend to be a help desk technician, or an agency user (especially an upper-level manager or other "authority figure") who urgently needs access to a particular system. If you give out your password, you are allowing the hacker an easy way into the system!

PASSWORD GUIDANCE

Passwords are the keys to your system. Therefore, they should be carefully chosen and protected.

- ! Passwords and computer usernames/userids **shall not** be shared with other users.
- ! Temporary passwords should be changed as soon as possible.
- ! Passwords should be at least eight characters long if possible.
- ! The password **must not** be the same as, or similar to, the username/userid.
- ! Random combinations of numeric, alphabetic, and special characters (if allowed by your system) furnish a more complex, and therefore more secure, password. Using uppercase and lowercase is recommended if your system accepts both.
- ! Passwords should never be composed of personal data that someone who knows you could guess, such as your name, your spouse's, child's, or pet's name, your birthday, street address, telephone number, favorite sports team or car, etc.
- ! Agency, organization, or project acronyms must not be used as passwords.
- ! Passwords should also not be a word found in a common dictionary (which makes them vulnerable to a "dictionary attack"), especially obvious words such as "password," or commonly used and guessed phrases such as "topsecret" or "superuser."
- ! Passwords **must not** be posted on the computer, monitor, partition, wall, etc. If a password must be recorded, it should be sealed in an envelope and locked in a desk, file drawer, or safe.

SECURITY REMINDER - PROTECTING LAPTOP COMPUTERS

All employees and contractors with laptop computers are reminded to protect them and their data from theft and damage. An estimated 319,000 laptops were reported stolen in 1999, with insurance claims totaling \$800,446,000. Security guidelines and best practices include:

Do not put classified information on a laptop computer without proper approval (see FSA Notices IRM-313, Protecting Classified Information, and IRM-307, Information Systems Security Program).

Do not use an automatic logon program (a program containing both the computer logon identification and password) on the laptop. This will prevent exposing the Government's computer system to unauthorized access if the laptop is lost or stolen.

The top three ways laptop computers are damaged are: dropping it; dropping something on it; and spilling a liquid on it. Avoid exposure to extreme temperatures and magnetized devices. Magnetic fields may destroy the software and data files.

All employees and contractors who travel must be alert at all times to protect the laptop from theft, especially in the airport, train station, rental car office, and hotel. **Do not** check a laptop as baggage; keep it with you at all times. Do not put the laptop in the overhead compartment since it may fall out when the compartment is opened. The laptop and the data stored on diskettes **will not** be damaged by exposure to airport x-ray machines.

Laptops are frequently stolen at airports. Two methods of laptop theft at the airport usually involve two thieves. The first method occurs when you are at the x-ray machine. The first thief precedes you through the security check point and then stands by the area where the carry-on luggage comes off the x-ray machine's conveyor belt. When you place your laptop computer onto the conveyor belt, the second thief steps in front of you and sets off the metal detector. While you are delayed, the first thief removes your laptop from the conveyor belt, and quickly disappears. The second method occurs when you are walking through a crowd and carrying the laptop on a luggage carrier. The first thief stops abruptly in front of you. When you stop, a second thief behind you takes your laptop and disappears into the crowd.

Keep a close eye on the laptop as it travels through the x-ray machine. **Do not** place it on the conveyor belt before you are ready to pass through the metal detector. Retrieve the laptop immediately after it goes through the x-ray machine.

Do not leave the laptop unattended anywhere such as: the office, car, taxi, bus, airport, train station, rental car office, and hotel. A good security rule is to never let the laptop out of your sight unless it is locked up. When staying in a hotel, never leave a laptop in the room unattended; if the room or hotel has a safe available, keep it there. When traveling, keep it in your hand or strapped to your shoulder. The laptop can be replaced, but the data stored on its hard disk may not. Always make backups of software and data files on the laptop for disaster recovery purposes. **Do not** store the backups with the laptop.

If your FFAS laptop is lost or stolen, you must report it immediately to your supervisor and an Information Systems Security Officer for investigative purposes. Always keep identification information about the laptop such as: serial number, make, and model with you separately, back at your office, and at home, for reporting purposes.

COMPUTER VIRUS DETECTED - WHO TO CALL

If you detect a computer virus on your PC or LAN, please call the help desk contact number listed below:

Location	Contact
Headquarters, Washington, DC-FSA and RMA users	202-690-4316
Headquarters, Washington, DC-FAS users	202-720-6763
2101 L Street, NW (Washington, DC)	202-418-9070
Park Center (Alexandria, VA)	703-305-1404 or 703-305-1406
Portals Building (Washington, DC)	202-720-2689
FAS Posts	202-720-2944
FSA Kansas City, MO and St. Louis, MO Offices	816-926-6897 or 816-926-6537
FSA Field Offices	800-255-2434 or 816-926-6537
RMA Kansas City, MO and Field Offices	816-926-1126

If you want more information on computer viruses and worms, please access the following web sites:

<http://www.F-secure.com/v-descs/>

<http://vil.nai.com/vil/default.asp>

<http://www.symantec.com/avcenter/vinfodb.html>

NOTE: If users receive an E-mail message warning them about a security problem, especially a computer virus, they should forward the message to their local Information System Security Officer for review and investigation purposes. There are many messages sent to FSA, FAS, and RMA users about computer virus hoaxes. Users should not pass these messages on, but send them to their local Security Officer. If the message is valid and important, the security office will issue a security alert.

FOR MORE SECURITY INFORMATION: VISIT A FFAS SECURITY WEB SITE

For users behind the USDA firewall, please visit the FFAS Information Systems Security home page on the FFAS Washington, DC intranet at:

<http://dc.ffasintranet.usda.gov/security/sec-page1.html>

Computer security awareness information is available through the links on this page.

FSA users can visit the FSA Kansas City Information Systems Security home page on the FSA Kansas City and St. Louis intranet at:

<http://intranet.fsa.usda.gov/security>

FAS users (a userid and password for FASTnet, the FAS intranet, is required) can access FFAS Information Systems Security information at:

http://fastnet.usda.gov/ftss/briefing_book/security/security_news.htm

Computer security awareness information is available through links on this page or directly at:

<http://fastnet.usda.gov/ftss/itsd/security/security-awareness.html>

INFORMATION SYSTEMS SECURITY SUMMARY

Basic Rules of Computer Security:

- ! Restrict data and information access to authorized personnel only.
- ! Use only good passwords, change them frequently, and **DO NOT** share them with anyone.
- ! Log off (or password protect) and lock up when not using computer resources.
- ! Protect all computer and information resources (diskettes, equipment, reports, etc.) from physical hazards.
- ! Backup all data and files on your computer using tapes and diskettes for disaster recovery purposes and store all backup media in a secured place onsite and offsite. Files stored on a FFAS network are usually backed up regularly, but you may want to make your own backups of important files.
- ! Use only authorized and legal copies of software.
- ! Shred old sensitive reports and printouts.
- ! Lock file cabinets and your desk and keep it clean of sensitive material.
- ! Document any computer, information, and communications misuse, abuse, and security incident. Report it immediately to your immediate supervisor and your local Information Systems Security Officer. Please see **Appendix A** for a list of the Washington, DC and Kansas City, MO information systems security officials.

THANK YOU!

Employees are the Key to Good Security-You are the Key! Thank you for reading this awareness material. The appendices present a list of information security officials; questions and answers on limited personal use of the Internet and E-mail; and, for reference, a list of computer security laws, regulations, policies, etc.

APPENDIX A**FFAS INFORMATION SYSTEMS SECURITY PROGRAM OFFICIALS****FSA, FAS, and RMA Metropolitan Washington, DC Offices and FAS Field Offices**

USDA-FSA-ITSD-PPB-ADPTSSS STOP 0584
 1400 Independence Avenue SW
 Washington, DC 20250-0584

Brian J. Davies, FFAS Information Systems Security Program Manager (202) 720-2419
 FAX: (202) 720-7134

Seabelle J. Ball, Information Systems Security Officer (202) 205-7399
 Patricia B. Gray, Information Systems Security Officer (202) 720-2599
 Eric M. Miller, Information Systems Security Officer (202) 720-0146
 Sue Weis, Information Systems Security Officer (202) 690-4639
 Roger W. Scaife, Deputy Information Systems Security Officer (202) 720-9152

FSA KC Office, FSA Field Offices, Farm Loan Program Offices in St. Louis, MO, RMA Offices in Kansas City, MO, and RMA Regional Services Offices, and Compliance Offices Agency-Wide

USDA-FSA-KCITSTO-ISSPS STOP 9198
 6501 Beacon Drive
 Kansas City, MO 64133-4676

Tony J. Capo, FSA KC Office Information Systems Security Program Manager (816) 926-1485
 FAX: (816) 926-6090

**FSA KC Office Information Systems Security Help Desk
 (Staffed by three Contract Employees)**

(816) 926-6537
FAX: (816) 926-6090

Linda N. Allen, Information Systems Security Officer (816) 823-1070
 Janell S. Duke, Information Systems Security Officer (816) 926-1641
 Noah W. Edmeier, Information Systems Security Officer (816) 823-1995
 Mindy J. Gehrt, Information Systems Security Officer (816) 926-7323
 Jerry D. Hall, Information Systems Security Officer (816) 926-6290
 Kurt R. Hoffman, Information Systems Security Officer (816) 926-3709
 Marcia A. McCarty, Information Systems Security Officer (816) 926-3024
 Gail S. Phillips, Information Systems Security Officer (816) 823-1818
 Andrew K. Solomon, Information Systems Security Officer (816) 926-6910

RMA KC Office Information Systems Security Help Desk

(816) 926-7320

FAX: (816) 926-6460

Karen A. Grissom, Information Systems Security Officer (816) 926-1341
 Helen M. Morris, Information Systems Security Officer (816) 926-2730

APPENDIX B**FFAS INTERNET AND ELECTRONIC MAIL (E-MAIL) POLICY OVERVIEW**

<i>Commonly Asked Questions</i>	<i>Guidelines to Follow</i>	<i>General Comments</i>
1. May I use a private Internet Service Provider (ISP) such as AT&T or America Online (AOL) from my office work station to access the Internet during business hours or on my own time?	No. All access to the Internet must be through the USDA Internet Access Network. No private Internet Service Providers such as AOL are allowed.	Provisions have been established for special testing scenarios at development centers of WEB pages. However, a waiver from the Security Office to the Department is required.
2. What type of equipment does Notice IRM-306 address?	Telephones, facsimile (FAX) machines, electronic messaging, computer equipment, E-mail, and the Internet.	
3. Do I need any special permission to use Government equipment for limited personal use on my own time?	Yes. Employees must request "limited use access" from their immediate supervisor for specific time frames, such as before or after work and/or during specified lunch periods and/or breaks to use the Internet for personal use. The supervisor can approve or deny the request.	It's the supervisor's decision if the supervisor wants the request verbally or in writing. The limited personal usage must comply with the intent of Notice IRM-306. Supervisors should make sure that all employees and contractors have access to this IRM Notice and are strongly encouraged to read it.
4. May I use government-owned equipment any time I want after hours for limited personal usage?	No. If employees choose to use Government equipment before and/or after work hours, it should conform to reasonable building opening and closing times to insure all building security regulations are followed and the Government incurs no additional cost. For example, if the normal business hours of operation at the employee's workplace are from 6:00 A.M. to 8:00 P.M., it is not reasonable to allow employees to come in earlier than 6:00 A.M. or stay later than 8:00 P.M. just to use Government equipment for limited personal use.	Buildings or separate offices that have 24-hour guard services would follow normal building security regulations of signing in and out after hours. Most Government offices have posted standard business hours of operation. Use of Government equipment outside these hours is by permission only. Union agreements clearly define normal Government business hours for a standard workday.

<i>Commonly Asked Questions</i>	<i>Guidelines to Follow</i>	<i>General Comments</i>
5. May my immediate family members or friends use the Government equipment after hours?	No. Only Federal employees and assigned contractors are allowed to use Government equipment for limited personal use.	
6. May contractors use Government equipment for limited personal use?	Yes. Contractors are governed by the same set of rules as Government employees. However, prior permission for use must come from the Contracting Officer's Representative (COR) or Contracting Officer's Technical Representative (COTR) that they are governed by.	The letter of the contract and statement of work is always the determining factor for contractors and this privilege will be disallowed if so stated in the contract language.
7. What are some specific things that I cannot do while using the Internet or E-mail for limited personal use?	Some examples of items that you cannot do: <ul style="list-style-type: none"> ▪ Run a private business. ▪ Use the equipment as a staging ground or platform to gain unauthorized access to other systems. ▪ Create copy, transmit, or retransmit chain letters or other mass mailings regardless of subject matter. ▪ Solicit, advertise or sell items such as using eBay or running a real estate office. ▪ Send electronic messages containing discriminatory language or remarks that may constitute sexual harassment ▪ Use sexually explicit materials or remarks that ridicule other coworkers on the basis of race, creed, religion, color, sex, handicap, national origin, or sexual orientation. ▪ Earn outside income. ▪ Cause congestion, delay or disruption of services to any Government systems or equipment such as sending Greeting cards, videos, sound, or other large file attachments. 	There are several obvious things for which Government equipment should not be used. However, most of the prohibited areas are a matter of common sense.

<i>Commonly Asked Questions</i>	<i>Guidelines to Follow</i>	<i>General Comments</i>
8. Can anyone see what I am doing when I send E-mail messages or use the Internet?	<p>Yes. Monitoring tools are in place for Security and Telecommunication administrators to monitor all access to the Internet and E-mail.</p> <p>By using Government office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet, and using E-mail.</p>	<p>USDA DR 3300-1 states those employees and contractors do not have a right, nor should they have an expectation, of privacy while using Government office equipment at any time.</p> <p>Departmental and Agency Officials may access E-mail messages whenever there is a legitimate Governmental purpose for such access. System administrators and other personnel with special system level access privileges are expressly prohibited from reading the E-mail of others unless authorization has been granted by senior management officials.</p>
9. May I bring games (CD's or diskettes) from home?	No. Playing games in the workplace during or after business hours is prohibited.	You may bring music CD's from home and play at work as long as the noise does not disrupt the workplace or other employees. Earphones or headsets are strongly encouraged.
10. May I download games from the Internet and play them?	<p>No. You may not load games on your hard drive of your PC anytime. Playing games on-line is prohibited.</p> <p>In addition, creating, downloading, viewing, storing, copying or transmitting materials related to illegal gambling, illegal weapons, and any other illegal activities are strictly prohibited.</p>	Loading "nonstandard" software on any Government PC can raise questions of compatibility. Your software can conflict with one or more Government applications and cause PC and/or network problems. The presence of nonstandard software on a PC makes Tech support difficult if not impossible.
11. May I make personal banking transactions using the Internet on my own time?	Yes. If your bank has a WEB site that can be accessed online, you may make normal banking transactions that you normally would be allowed to do by phone.	<p>You must obtain limited user access permission from your supervisor.</p> <p>You cannot load banking software on your PC.</p>

<i>Commonly Asked Questions</i>	<i>Guidelines to Follow</i>	<i>General Comments</i>
<p>12. May I use Government equipment on my own time to copy special flyers for charitable clubs or nonprofit organizations that I belong to such as, Scouts, School or Parent-Teacher Association (PTA), or for my own home use?</p>	<p>Yes. You may make a very limited number of copies of documents as long as these clubs or events are nonprofit and no service fee is being charged.</p> <p>USDA sponsored or work-sponsored teams such as USDA bowling and/or golf leagues may use Government equipment to print documents after hours as long as you are not being paid a salary for performing this activity.</p> <p>Also, there must be minimal additional expense to the Government.</p> <p>The intent is not for the Government to subsidize printing costs for non-work related ventures of any kind.</p>	<p>You cannot store these personal files on Government equipment.</p> <p>Personal diskettes should be personally procured and virus checking on diskettes needs to be completed prior to using.</p> <p>You should obtain limited user access permission from your supervisor.</p>
<p>13. May I buy and sell stock on-line on my own time?</p>	<p>No. Telecommunications resources and official time shall not be used to earn outside income. Therefore, these types of activities cannot be performed during working or non-work hours.</p> <p>However, you may make changes on-line to your Thrift Savings Plan (TSP) accounts.</p>	<p>The intent of this privilege is to allow some limited management of your personal TSP retirement funds and was not intended to support daily stock trading.</p>
<p>14. May I use Government equipment to print special documents for sports teams and other for-profit clubs that I belong to?</p>	<p>No.</p> <p>The intent is not for the Government to subsidize printing cost for non-work related ventures of any kind</p>	<p>See item 12 above.</p>
<p>15. Will I get in trouble if I violate these regulations identified in Notice IRM-306?</p>	<p>Yes. Up to and including dismissal depending on the severity of the offense.</p>	<p>The immediate supervisor with input and guidance from FSA's Human Resources Division (in Washington, DC) or FSA's Personnel Division (in Kansas City, MO) Employee Relations Specialists decides punishment.</p>

<i>Commonly Asked Questions</i>	<i>Guidelines to Follow</i>	<i>General Comments</i>
16. What are the rules for downloading software from the Internet?	<p>Downloading software is not permitted whether it's free or not.</p> <p>You cannot download software from the Internet or bring software in from outside of USDA that violates the copyright on the software and/or makes FSA, FAS, or RMA liable for violation of the Copyright Act.</p>	<p>You cannot use sites such as bluemountain.com to receive birthday and get well cards from employees or friends. You may send these types of cards to non-Government employees and friends.</p>
17. May I use the telephone for personal business?	<p>Yes. Limited personal use is allowed as long as it does not generate more than minimal expense to the Government.</p>	<p>Long distance personal calls are prohibited. Length of local calls should be kept at a minimum.</p>
18. Are personal E-mail messages allowed to be sent and received at work?	<p>Yes. You may send and receive E-mail messages within reason to and from non-business addresses.</p> <p>However, you are not allowed to establish personal E-mail accounts at work using Hotmail, Yahoo, etc. (FAS may allow exceptions for overseas posts).</p>	<p>You are not allowed to forward your personal ISP E-mail to your Government E-mail account.</p> <p>All E-mail, both business related and personal, would be stored and backed up nightly on the Agency network.</p>
19. May I customize my background wallpaper and pattern on my PC?	<p>Yes. Changing the background wallpaper and pattern are not considered to be configuration changes.</p> <p>However, employees are guided by the code of ethics and conduct and must adhere to all polices regarding offensive materials in the workplace.</p>	<p>Pictures of family, animals, and other normal acceptable business office type pictures are ok.</p> <p>Pictures of scantily clad males or females or other pictures covered under sexual harassment policy are prohibited. See your supervisor for final determinations.</p> <p>Supervisors will direct the users to remove inappropriate or offensive wallpaper immediately from all Government equipment.</p>
20. May I download screen savers from the Internet or bring a CD of Screen savers from home and load it on my PC or laptop?	<p>No. You may not download screen savers or any other file from the Internet.</p> <p>However, you may capture any appropriate graphic image for use as a screen saver or wallpaper from non-Government sources within the guidelines of item 19. above.</p>	<p>Installing a screen saver is considered a configuration change to the equipment and is known to cause resource problems.</p>

<i>Commonly Asked Questions</i>	<i>Guidelines to Follow</i>	<i>General Comments</i>
21. May I use the FAX machine for personal use?	Yes. Within common sense and limited boundaries, you may send a fax to local (not long distance) telephone numbers for personal business.	You should obtain limited user access permission from your supervisor.
22. May I read such things as the newspaper, check the weather, look at new car web sites, and other nonrestrictive sites on the Internet on my own time?	Yes. You may also access magazines and other reference materials not blocked or identified as offensive. You may research and review any business-related materials on the Internet during work hours as directed by your supervisor.	You must obtain limited user access permission from your supervisor for non-business related usage.
23. Is the Agency looking at new technology on the Internet such as allowing parents at work to use the Internet to check on their children at daycare?	Yes. A number of daycare centers have installed cameras that are connected to the Internet to allow parents to observe their children during the day from their work computers as part of the family friendly initiative.	Employees would be allowed to check on children using the Internet once or twice a day, but should not leave this connection continuously open on their desktops. These types of Web Sites are major resource hogs and can easily overburden a network if they are kept up continuously. You should obtain limited user access permission from your supervisor.
24. If I have specific questions on Computer Security related issues, who should I call for clarification?	Please contact your local State Office or Headquarters security office. All official security policies and regulations are issued by the FFAS Information Systems Security Office and enforced by the FFAS Information Systems Security Program Staff in Washington, DC and Kansas City, MO.	Each State Office should identify an onsite security official and a backup to address security-related issues and to coordinate responses with Headquarters as needed. Violations should be reported to the onsite security officer, who in turn would coordinate with Headquarters security and personnel specialists.

As a reminder, users should be aware that personal information that traverses the Internet and Intranet is not secure and data integrity cannot be guaranteed. Also, the Government is not responsible in any way for personal data that is "sniffed" (via a Network Protocol Analyzer, commonly known as a "sniffer") from the Internet or the intranet and used for unauthorized personal gain or embarrassment to the user. Users use the Internet at their own risk for personal business.

This short overview is intended for managers, supervisors, and employees to use as a guideline for managing and enforcing Notice IRM-306. It is not intended to override or replace this Notice. It also is not intended to override or replace the Standards of Ethical Conduct for Employees of the Executive Branch handbook, codified in Title 5, Code of Federal Regulations, Part 2635 (5 CFR 2635). It should be used as a question and answer document to help clarify the intentions of Notice IRM-306.

If you want more information, please see the following:

- ! FSA Notice IRM-306, FFAS Internet and Electronic Mail (E-Mail) Policy, available at:
<http://www.fsa.usda.gov/dam/forms/notices.asp>
- ! USDA DR 3300-1, Telecommunications and Internet Services and Use, available at:
<http://www.ocio.usda.gov/irm/directives/index.html>
- ! The “Using Government Property and Time” training module at USDA’s Office of Ethics web site at:
<http://www.usda.gov/ethics/training>
- ! Standards of Ethical Conduct for Employees of the Executive Branch at the U.S. Office of Government Ethics web site at:
http://www.usoge.gov/pages/forms_pubs_otherdocs/fpo_files/reference/rfsoc_99.pdf
- ! The Code of Federal Regulations (CFR), available at:
<http://www.gpo.gov/nara/cfr/index.html>

APPENDIX C

COMPUTER SECURITY FEDERAL LAWS, EXECUTIVE ORDERS, REGULATIONS (GOVERNMENT-WIDE, USDA, AND DEPARTMENT OF STATE), AGENCY POLICIES, AND GUIDANCE

The following Federal laws, executive orders, regulations, agency polices, and guidance apply to computer security in FFAS (this is not a complete list):

FEDERAL LAWS

- ! Children's Online Privacy Protection Act of 1998 (Pub. L. 105-277)
- ! Clinger-Cohen Act of 1996 (Division E of Pub. L. 104-106), formerly known as the Information Technology Management Reform Act
- ! Computer Fraud and Abuse Act of 1986 (Pub. L. 99-474)
- ! Computer Matching and Privacy Protection Act of 1988 (Pub. L. 100-503)
- ! Computer Security Act of 1987 (Pub. L. 100-235)
- ! Copyright Act, United States Code (U.S.C.), Title 17
- ! Electronic Communications Privacy Act of 1986 (Pub. L. 99-508)
- ! Electronic Freedom of Information Act Amendments of 1996 (Pub. L. 104-231)
- ! Electronic Signatures in Global and National Commerce Act ("E-SIGN") of 2000 (Pub. L. 106-229)
- ! Federal Managers' Financial Integrity Act of 1982 (Pub. L. 97-255)
- ! Federal Records Act (44 U.S.C. 3101)
- ! Freedom of Information Act (5 U.S.C. 552)
- ! Freedom to E-File Act of 2000 (Pub. L. 106-222)
- ! Government Information Security Reform Act (GISRA) of 2000 (Pub. L. 106-398, Subtitle G)
- ! Government Paperwork Elimination Act (GPEA) of 1998 (Pub. L. 105-277, 44 U.S.C. 3504)
- ! Government Performance and Results Act (GPRA) of 1993 (Pub. L. 103-62)
- ! National Infrastructure Protection Act of 1996 (Pub L. 104-294)
- ! Paperwork Reduction Act of 1980 (44 U.S.C. Chapter 35), as Amended by the Paperwork Reduction Act of 1995 (Pub. L. 104-13)
- ! Patent and Trademark Laws (U.S.C. Title 35)
- ! Privacy Act of 1974 (Pub. L. 93-579, 5 U.S.C. 552a), July 14, 1987
- ! Records Management by Federal Agencies (44 U.S.C. 3101-3107)
- ! Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as Amended by the Workforce Investment Act of 1998 (Pub. L. 105-220), August 7, 1998
- ! Title 18 U.S.C. 1902, Disclosure of Crop Information and Speculation Thereon
- ! Title 18 U.S.C. 1905, Disclosure of Confidential Information Generally
- ! Trade Secrets Act (18 U.S.C. 1905).

If you want more information on Federal Laws, please access the following web sites:

http://www.firstgov.gov/Topics/Reference_Shelf.shtml#laws

<http://thomas.loc.gov>

If you want more information on the United States Code (U.S.C.), please access the following web site:

<http://uscode.house.gov>

EXECUTIVE ORDERS AND PRESIDENTIAL DECISION DIRECTIVES

- ! Executive Order 10450 of April 27, 1954, Security Requirements for Government Employment, as amended
- ! Executive Order 12958, April 17, 1995, Classified National Security Information, as amended by Executive Order 13142, Amendment to Executive Order 12958-Classified National Security Information, November 19, 1999
- ! Executive Order 13011, Federal Information Technology, July 16, 1996
- ! Executive Order 13103, Computer Software Piracy, September 30, 1998
- ! Presidential Decision Directive 63, Critical Infrastructure Protection, May 22, 1998
- ! Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001.

If you want more information on Executive Orders, please access the following web site:

<http://www.nara.gov/fedreg/eo.html>

If you want more information on Presidential Decision Directives, please access the following web site:

<http://www.loc.gov/rr/news/directives.html>

REGULATIONS

Government-Wide

- ! Office of Management and Budget (OMB) Circular A-123, Management Accountability and Control
- ! OMB Circular A-127, Financial Management Systems
- ! OMB Circular A-130, Management of Federal Resources, including Appendix III, Security of Federal Automated Information Resources
- ! OMB Memorandum M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records," January 7, 1999
- ! OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, June 2, 1999
- ! OMB Memorandum M-99-20, Security of Federal Automated Information Resources, June 23, 1999
- ! OMB Memorandum M-00-07, Incorporating and Funding Security in Information System Investments, February 28, 2000
- ! OMB Memorandum M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, April 25, 2000
- ! OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, June 22, 2000
- ! OMB Memorandum M-00-15, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act
- ! OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy, December 20, 2000
- ! OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, January 16, 2001
- ! OMB Memorandum M-02-09, Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones, July 2, 2002
- ! U.S. Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch.

REGULATIONS (continued)

If you want more information on Government-wide Regulations, please access the following web sites:

<http://www.whitehouse.gov/omb>

http://www.usoge.gov/pages/forms_pubs_otherdocs/fpo_files/reference/rfsoc_99.pdf

USDA

- ! USDA Departmental Manual (DM) 3140-1 Management ADP Security Manual
- ! USDA DM 3440-1, Classification, Declassification, and Safeguarding Classified Information
- ! USDA Departmental Regulation (DR) 3140-1, USDA Information System Security Policy
- ! USDA DR 3140-2, USDA Internet Security Policy
- ! USDA DR 3300-1, Telecommunications & Internet Services and Use
- ! USDA DR 3430-1 Home Page Development and Maintenance
- ! USDA DR 3440-1, Classification, Declassification, and Safeguarding Classified Information
- ! USDA Cyber Security Manual, Series 3500 and associated Cyber Security guidance (currently CS-001 through CS-020)
- ! USDA Office of Human Resources Management (OHRM) Personnel Bulletin 735-1, Employee Responsibilities and Conduct.

If you want more information on USDA directives, please see the following web sites:

<http://www.ocio.usda.gov/irm/directives/index.html>

http://www.ocionet.usda.gov/ocio/cyber_sec/policy.html (for Cyber Security Manual and guidance)

<http://www.usda.gov/ethics/rules/index.htm>

Department of State

Note: Department of State regulations apply to users at foreign posts and users connecting to Department of State systems.

- ! Department of State, Foreign Affairs Manual (FAM), Volume 12, Chapter 500 (12 FAM 500), Information Security
- ! Department of State, FAM, Volume 12, Chapter 600 (12 FAM 600), Information Security Technology
- ! Department of State, Foreign Affairs Handbook (FAH), 12 FAH-6, OSPB [Overseas Security Policy Board] Security Standards and Policy Handbook
- ! Department of State Cable issued May 1998, 98 STATE 083902, Overseas Storage of Classified Information, is an unclassified extract from 12 FAH-6, which is classified.

If you want more information on Department of State Foreign Affairs Manuals and Foreign Affairs Handbooks, please see the following web site. Note: Classified and Sensitive But Unclassified (SBU) materials are not included at the web site:

<http://foia.state.gov/FAMDir/FAM/fam.asp>

AGENCY POLICIES

The three policies below apply to FSA, FAS, and RMA:

- ! FSA Notice IRM-306, FFAS Internet and Electronic Mail (E-Mail) Policy
- ! FSA Notice IRM-307, Information Systems Security Program
- ! FSA Notice IRM-313, Protecting Classified Information.

The four Information Technology Working Group (ITWG) policies below apply to the County Based Agencies, i.e., FSA, Rural Development (RD), and the Natural Resource Conservation Service (NRCS):

- ! Computer Viruses and Related Threats Software Policy (Notice ITWG Security - 001)
- ! Background Investigations and Security Clearance Policy (Notice ITWG Security - 003)
- ! Computer Security Incident Response and Reporting Policy (Notice ITWG Security - 004)
- ! Computer Vulnerability Scan Policy (Notice ITWG Security - 005).

The policy below applies to FAS only:

- ! FAS Regulation, Title 8 Chapter 5 (8 FASR 5), Classification, Declassification, and Safeguarding Classified Information.

The policies below apply to RMA only:

- ! FCIC Information Systems Security Policy
- ! RMA Information Systems Security Handbook
- ! RMA Local Area Network (LAN) and Wide Area Network (WAN) Security Handbook.

If you want more information on FSA, FAS, and RMA directives, please see the following web site:

<http://www.fsa.usda.gov/dam/forms/notices.asp>

If you want more information on ITWG policies, they will be posted at the following web site, initially under the "News Flash" section:

<http://www.sci.usda.gov/cce/index.html>

GUIDANCE

The following Special Publications (SP) from the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) provide important computer security guidance:

- ! SP 500-166, Computer Viruses and Related Threats: A Management Guide, August 1989
- ! SP 500-169, Executive Guide to the Protection of Information Resources, 1989
- ! SP 500-170, Management Guide to the Protection of Information Resources, 1989
- ! SP 500-171, Computer Users' Guide to the Protection of Information Resources, 1989
- ! SP 800-4, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials, March 1992
- ! Draft SP 800-4A, Security Considerations in Federal Information Technology Procurements, October 2002
- ! SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995
- ! SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
- ! SP 800-16, Information Technology Security Training Requirements: A Role and Performance-Based Model, April 1998

- ! SP 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998
- ! SP 800-23, Guide to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, August 2000
- ! SP 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000
- ! SP 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001
- ! SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001
- ! SP 800-30, Risk Management Guide for Information Technology Systems, January 2002
- ! SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001
- ! SP 800-33, Underlying Technical Models for Information Technology Security, December 2001
- ! SP 800-34, Contingency Planning Guide for Information Technology Systems, June 2002
- ! Draft SP 800-35, Guide to IT Security Services, October 2002
- ! Draft SP 800-36, Guide to Selecting IT Security Products, October 2002
- ! Draft SP 800-37, Guidelines for the Security Certification and Accreditation (C&A) of Federal Information Technology Systems, October 2002
- ! SP 800-40, Procedures for Handling Security Patches, September 2002
- ! SP 800-41, Guidelines on Firewalls and Firewall Policy, January 2002
- ! Draft SP 800-42, Guideline on Network Security Testing, February 2002
- ! SP 800-43, Systems Administration Guidance for Windows 2000 Professional, November 2002
- ! SP 800-44, Guidelines on Securing Public Web Servers, September 2002
- ! SP 800-45, Guidelines on Electronic Mail Security, September 2002
- ! SP 800-46, Security for Telecommuting and Broadband Communications, September 2002
- ! SP 800-47, Security Guide for Interconnecting Information Technology Systems, September 2002
- ! SP 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, November 2002
- ! Draft SP 800-50, Building an Information Technology Security Awareness and Training Program, July 2002.

If you want more information on NIST computer security publications, please see the following web site:

<http://csrc.nist.gov/publications>

TO: USDA-FSA-Oklahoma
ATTN: Jan Courtright, Training Officer
100 USDA Suite 102 Stillwater, OK 74074-2653

SUBJECT: Certification of Completion - 2002 Annual Computer Security Awareness Training -
Required by May 30, 2003

I certify that I have received and read a copy of the electronic files containing the 2002 Annual Computer Security Awareness Training information. I understand that it is my continuing responsibility to become familiar with and abide by all applicable Federal laws and FFAS and USDA computer security regulations. In order to read the training material, I was given two hours of official time.

I further understand that I can get advice on computer security issues and questions from the officials listed in the training materials.

Training Office: Add this information to I-CAMS Course Number 020097 - Computer Security Training 2002.

Date Completed

FOR EMPLOYEES:

Employee's Name (Print or Type)

Employee's Signature

Employee's Social Security Number

NOTE: Your Social Security Number is required only for placing this receipt in your official training history.

Employee's Agency: **FSA**

Employee's County

Employee's Mailing Address

() _____
Employee's Telephone Number

FARM AND FOREIGN AGRICULTURAL SERVICES (FFAS) INFORMATION SYSTEMS SECURITY PROGRAM

TO: Farm Service Agency (FSA), Foreign Agricultural Service (FAS), and
Risk Management Agency (RMA) Employees and Contractors

GOOD COMPUTER SECURITY PRACTICES

Always Protect FFAS Information Resources - All classified, sensitive, private, and mission-critical information, data, systems, and applications require protection from unauthorized access, use, disclosure, alteration, and loss.

Know Our Policies - Read USDA, FFAS, FSA, FAS, and RMA directives, including FFAS Information Systems Security Program policies.

Protect Your Work Area - Recognize, politely challenge, and assist people who **DO NOT** belong in the work area.

Preventing Unauthorized Access - Computer resources and equipment, especially personal computers and servers, should not be exposed to unauthorized access.

Protect Passwords - Use only passwords which are not easily guessed or in the dictionary, change them frequently, and **DO NOT** share your password with anyone.

Protect Your Files - Establish and periodically review access privileges for each file.

Protect Your Computer - Always logoff or password protect your screen before leaving your computer system unattended. Always safeguard software and removable media such as diskettes.

Protect Against Computer Viruses - Never load unauthorized or personal software on your computer system. Report viruses immediately to your supervisor and the appropriate Help Desk for corrective action. Before loading data from any media (diskette, Internet, etc.), always check it for viruses.

Protect Against Disaster - Always have backup program, equipment, and databases ready to go.

Protect Classified and Sensitive Data and Information - Read USDA, FFAS, FSA, FAS, RMA and Department of State directives, policies, handbooks, and manuals. FAS classified information will be handled in accordance with the USDA, FFAS, FAS, and the Department of State regulations.

Report Violations - Document any computer and communications misuse, abuse, security incident or breach. Report it immediately to your supervisor and your Information Systems Security Officer.

DO YOU HAVE A COMPUTER SECURITY QUESTION OR NEED COMPUTER SECURITY ASSISTANCE?

Please contact your Information Systems Security Officer at:

Security Office at Kansas City Management Office in Kansas City, MO.

(816) 926-6537, (816) 926-1641, (816) 926-1341, or (816) 926-1458,

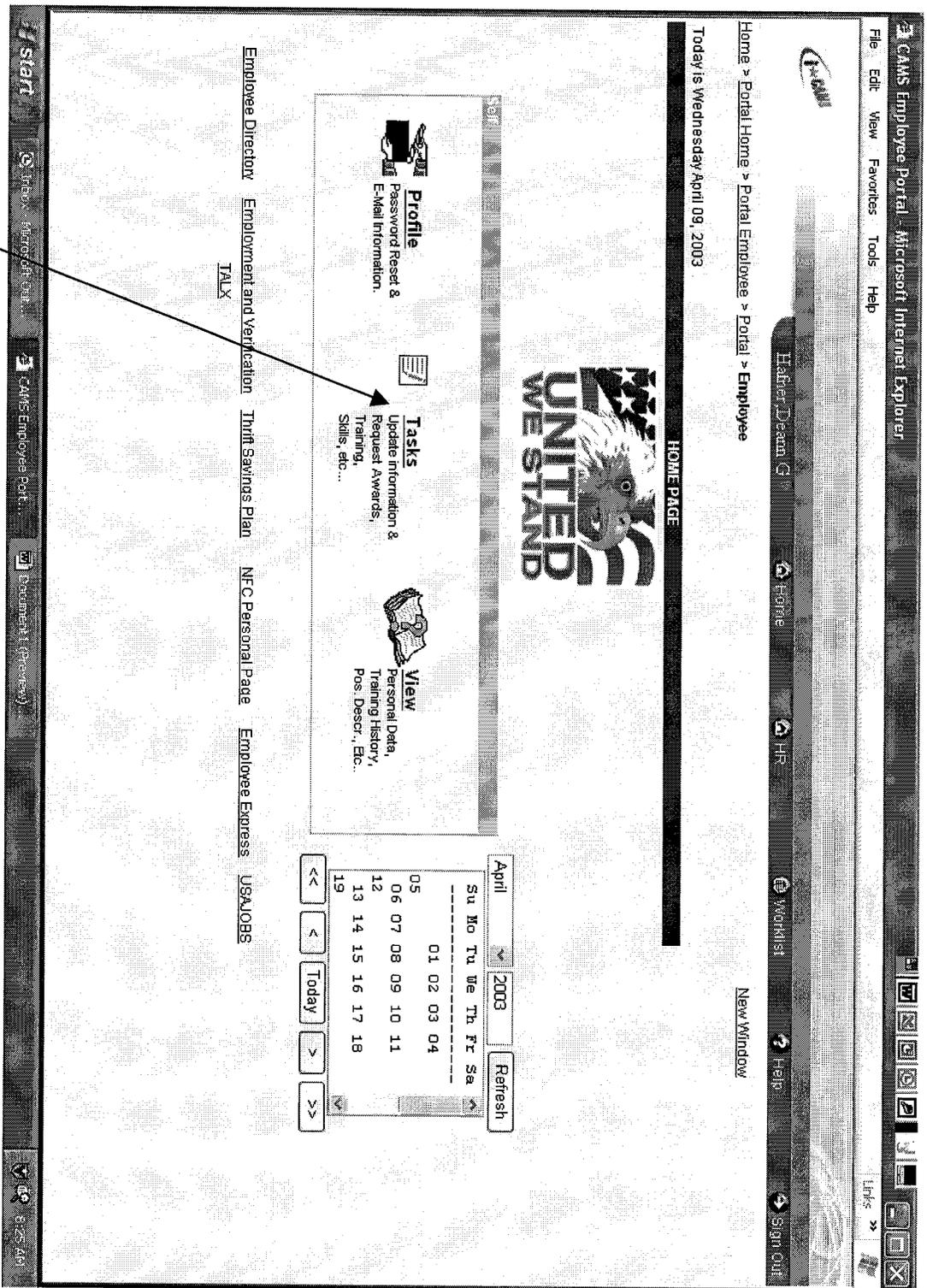
(816) 926-3018, or (816) 926-3709

Security Office at Headquarters in Washington, DC.

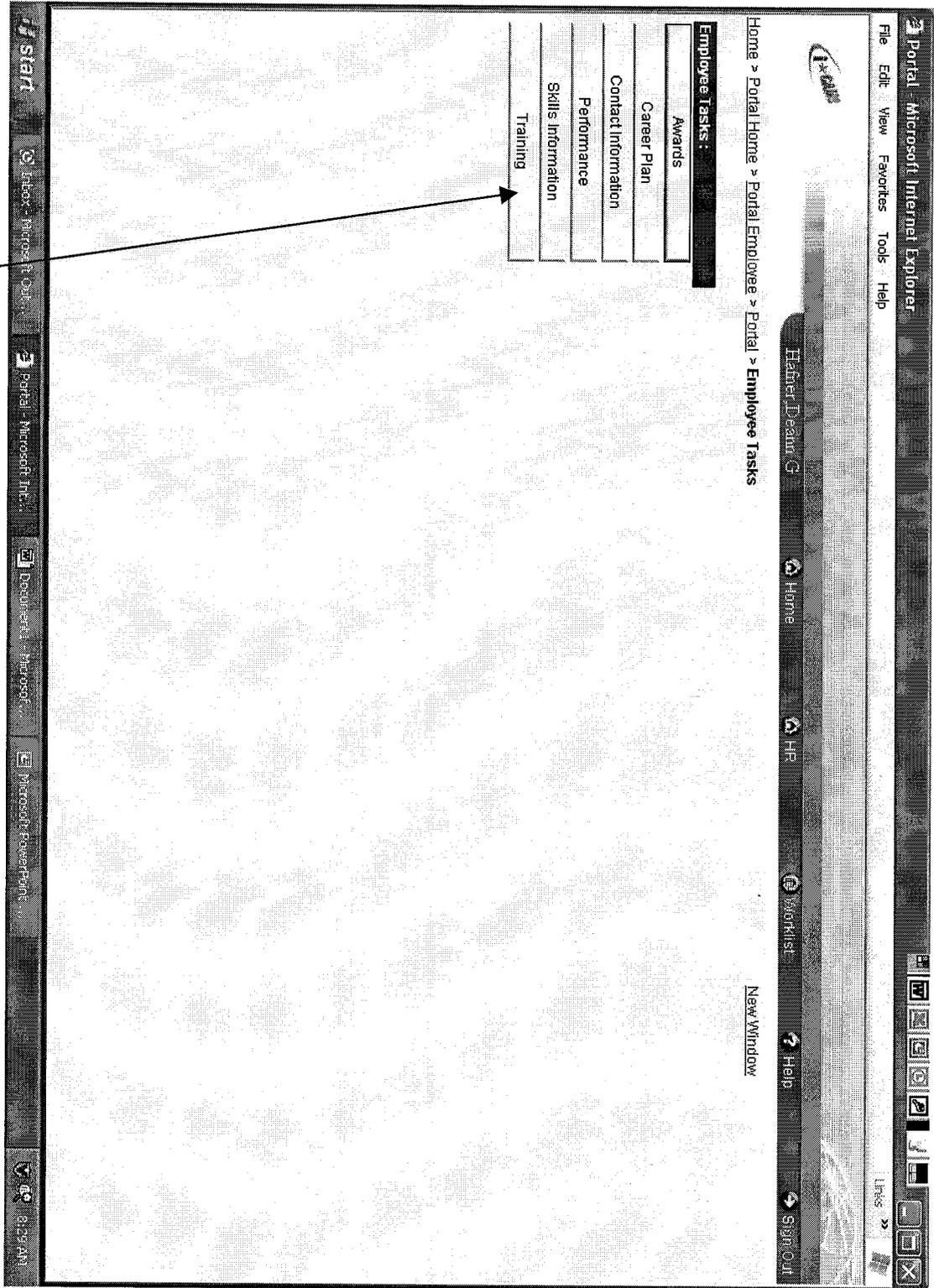
(202) 720-2419, (202) 720-6207, (202) 720-0146, (202) 690-2172, or (202) 205-7399

April 1999

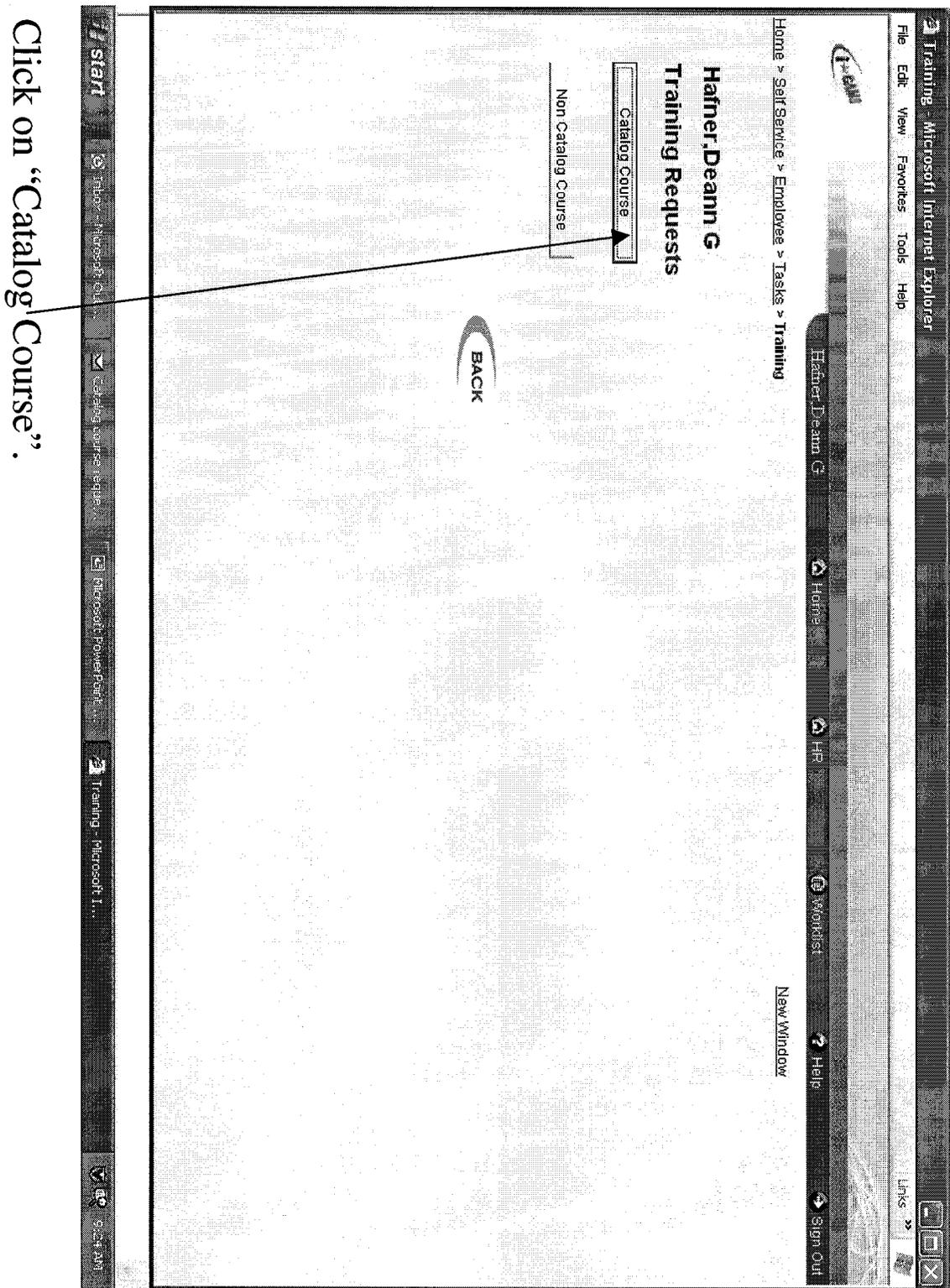
The following slides provide guidance for employees to certify completion of security awareness training by registering for ICAMS course number 020097



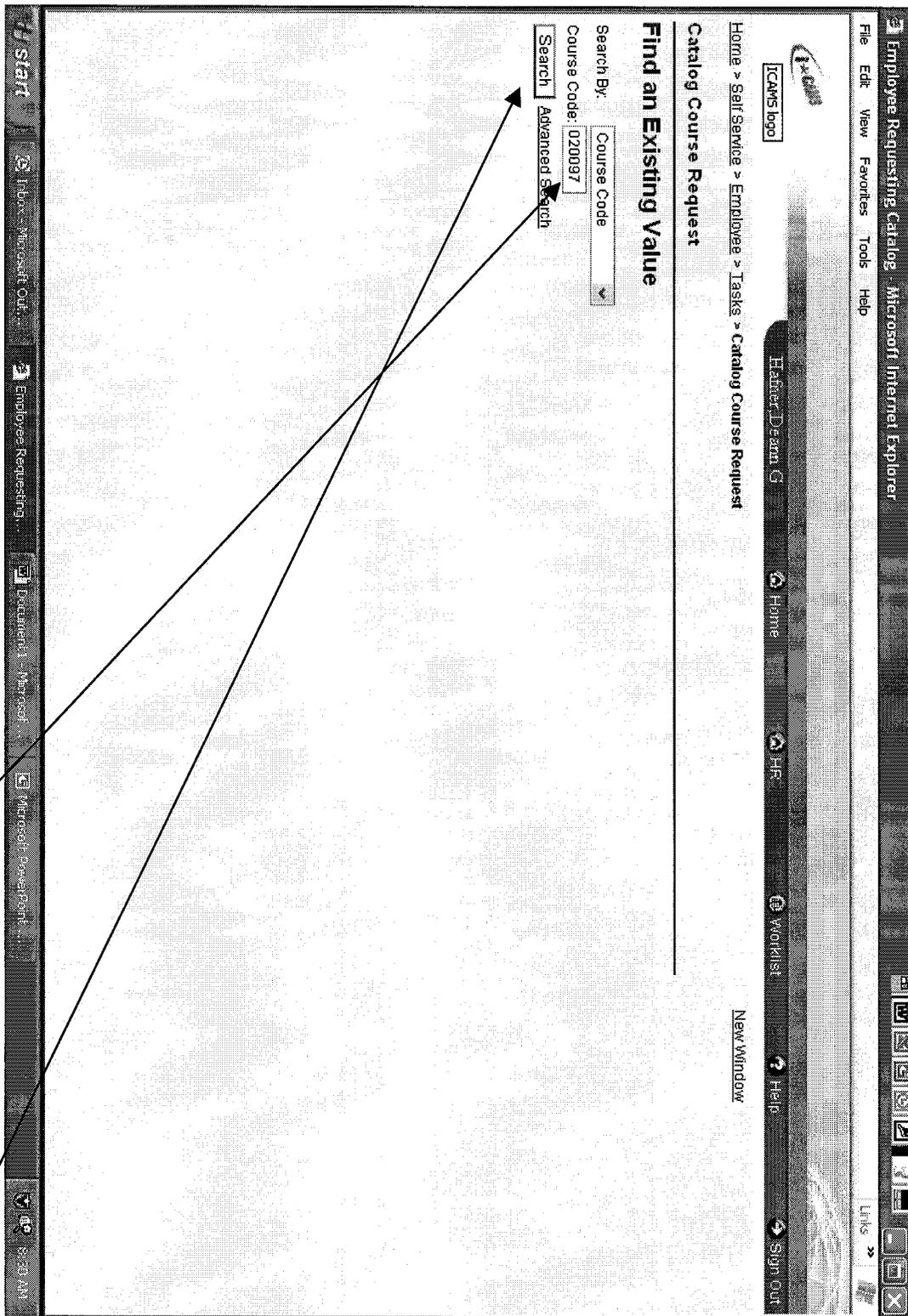
Click on "Tasks".



Click on "Training".

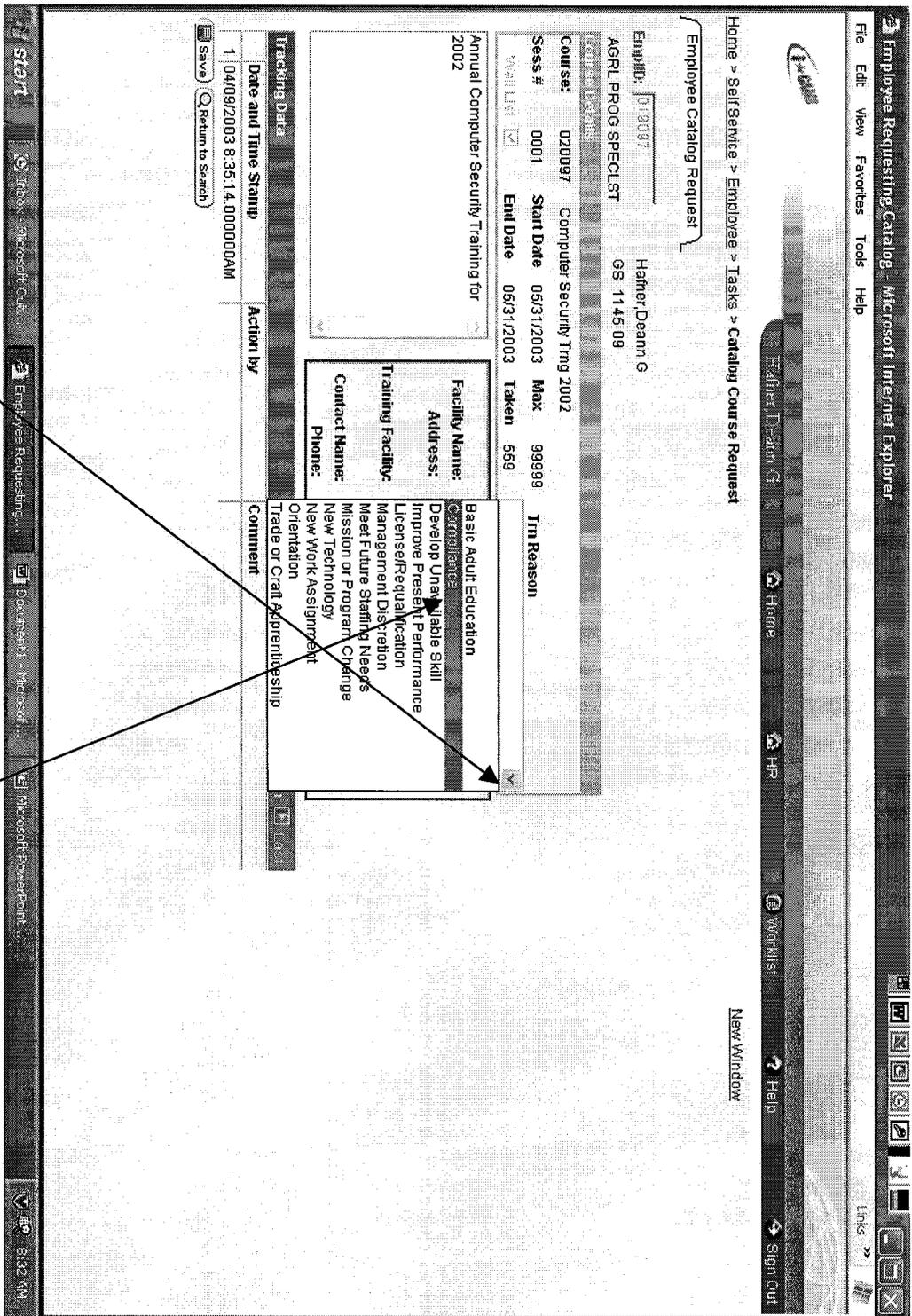


Click on "Catalog Course".



1. Type in the National ICAMS course number "020097" and, 2. Click on "Search".

04-09-03



- Click on the “down arrow” and, 2. Select “compliance” for the reason for the training.

Employee Requesting Catalog - Microsoft Internet Explorer

Home > Self Service > Employee > Tasks > Catalog Course Request

Employee Catalog Request

EmpID: 019997 Hamer, Deann G
AGRL PROG SPECLST GS 1145 09

Course: 020097 Computer Security Trng 2002
Sess # 0001 Start Date 05/31/2003 Max 99999 Trn Reason
End Date 05/31/2003 Taken 559 Confidential

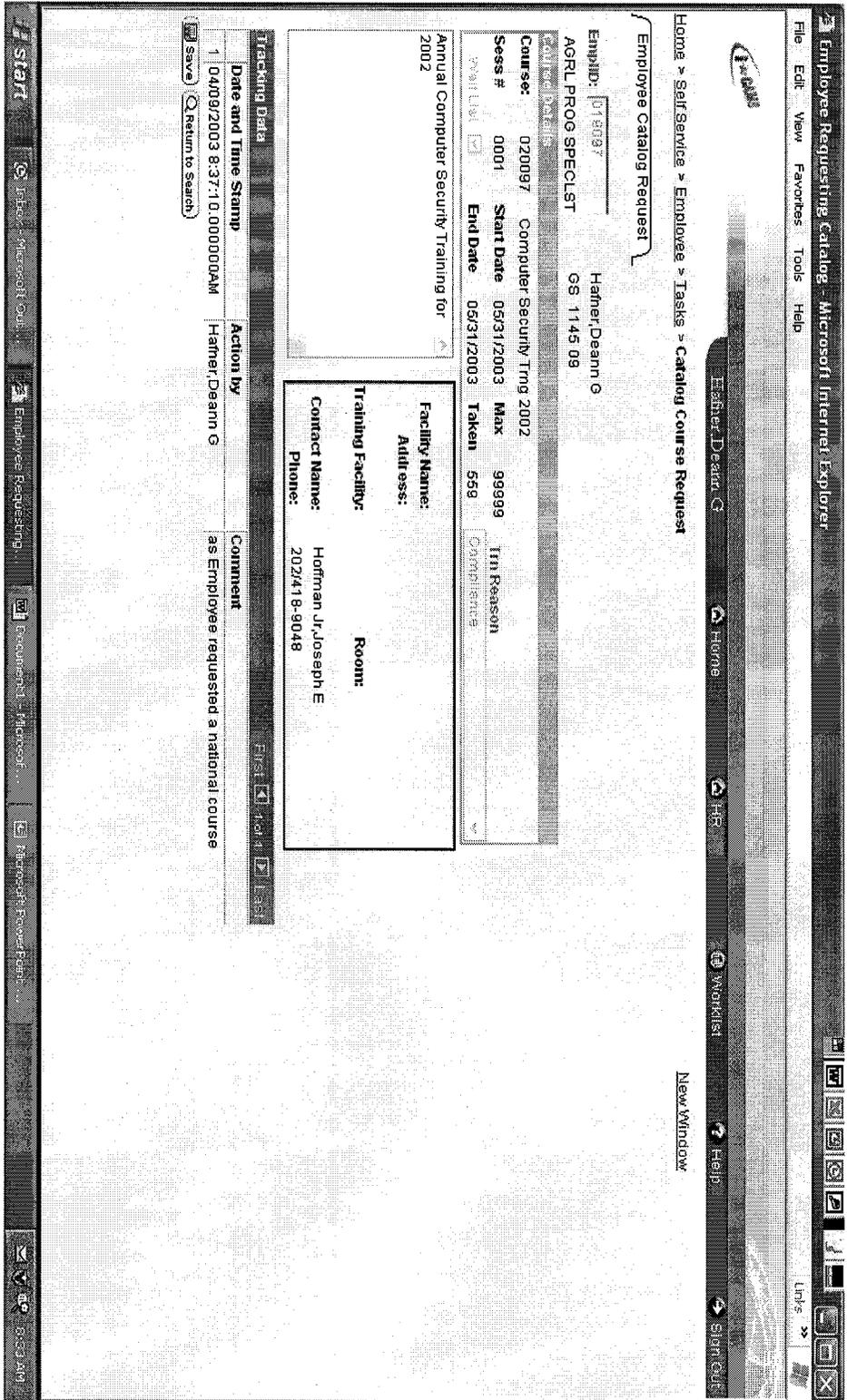
Annual Computer Security Training for 2002

Facility Name:
Address:
Training Facility: Room:
Contact Name: Hoffman Jr, Joseph E
Phone: 202418-9048

Tracking Date	Action by	Comment
1 04/09/2003 8:35:14 0000000AM		

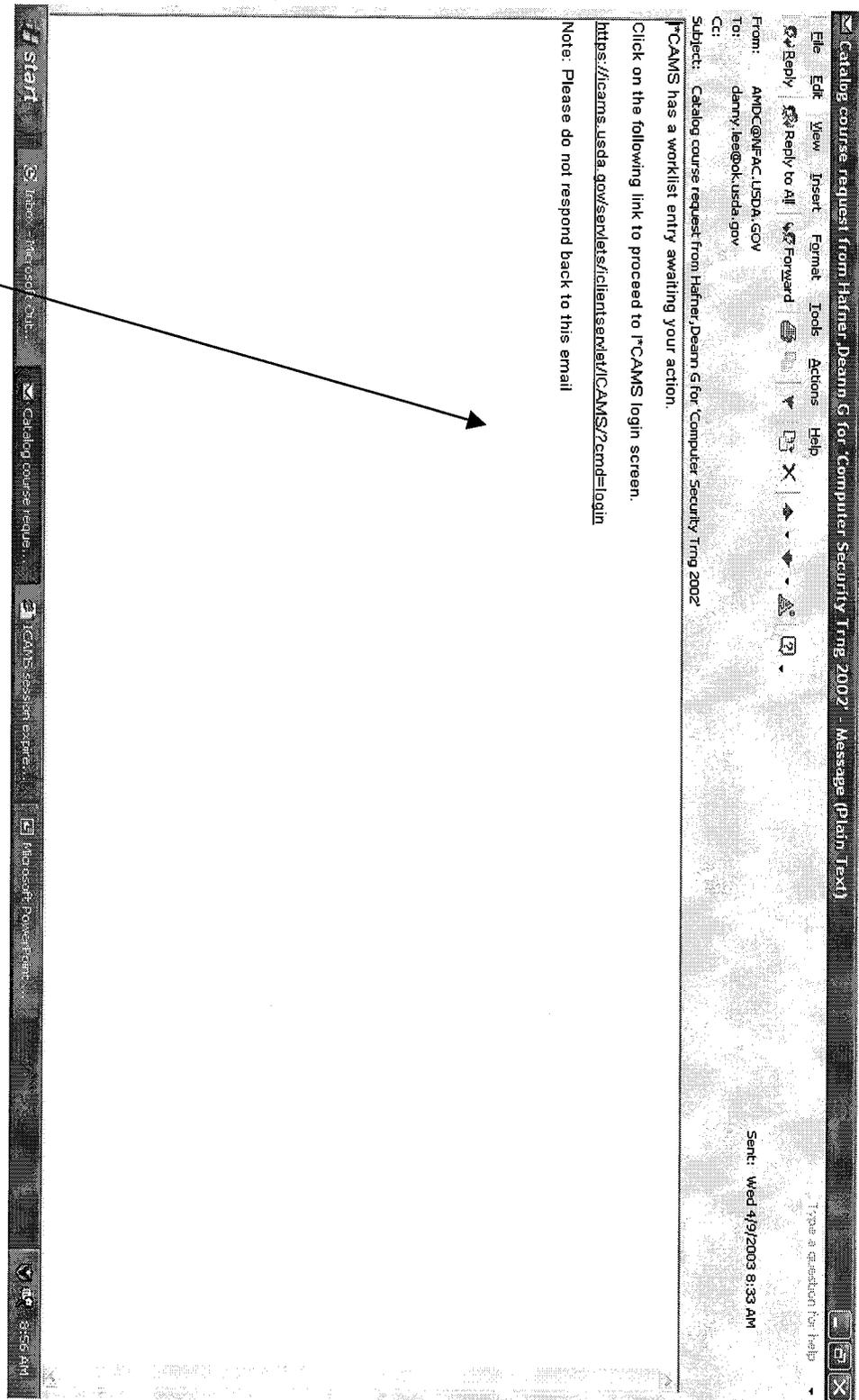
Save Return to Search

Remember to click on the "Save" button.

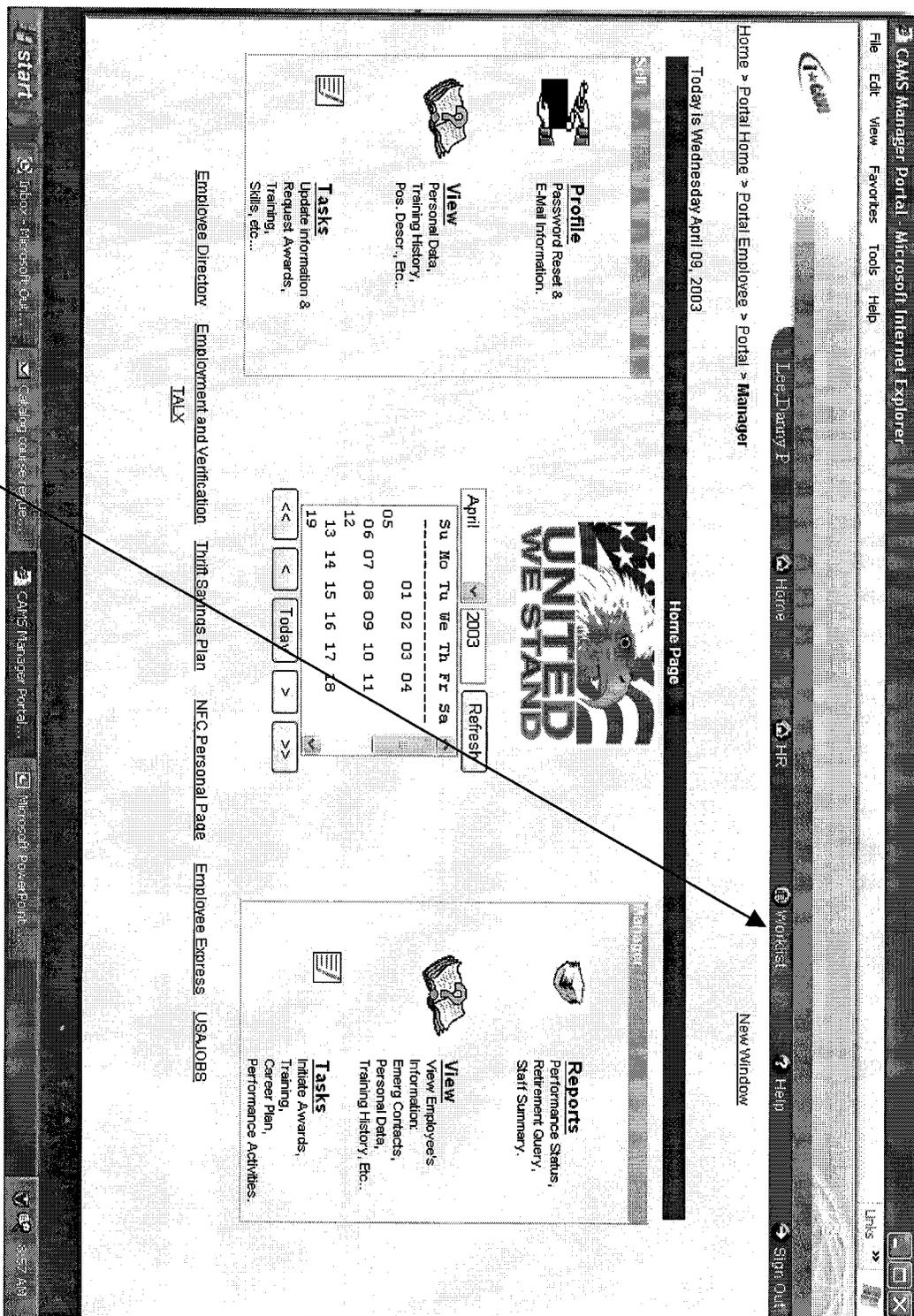


Note the tracking data after selecting "save". Your request will now flow to your supervisor's worklist for approval. Your supervisor will get an email informing him/her that he/she has a worklist item.

The following slides provide guidance for supervisors to approve (verify completion of security awareness training) through ICAMS for employees they supervise.

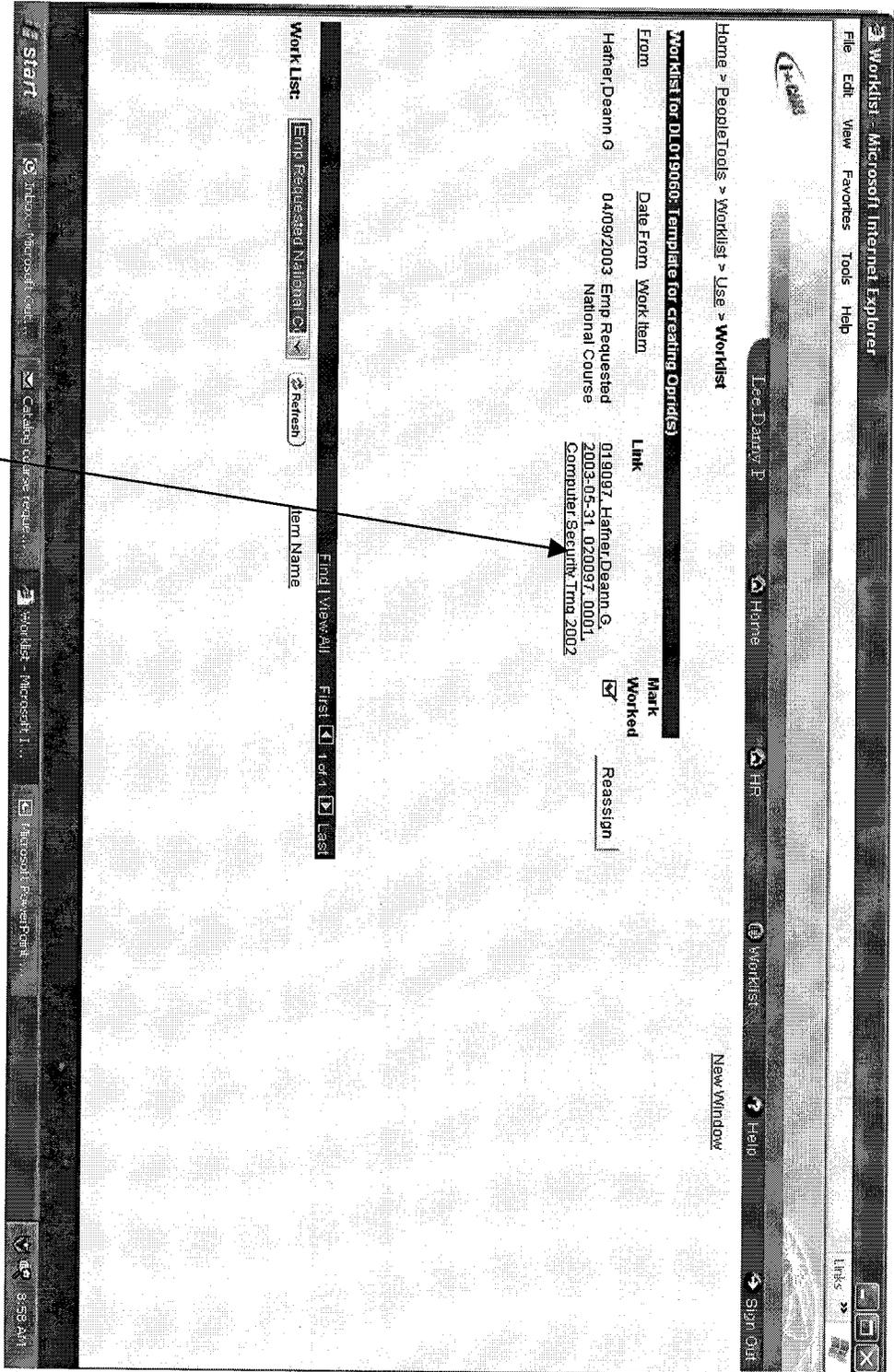


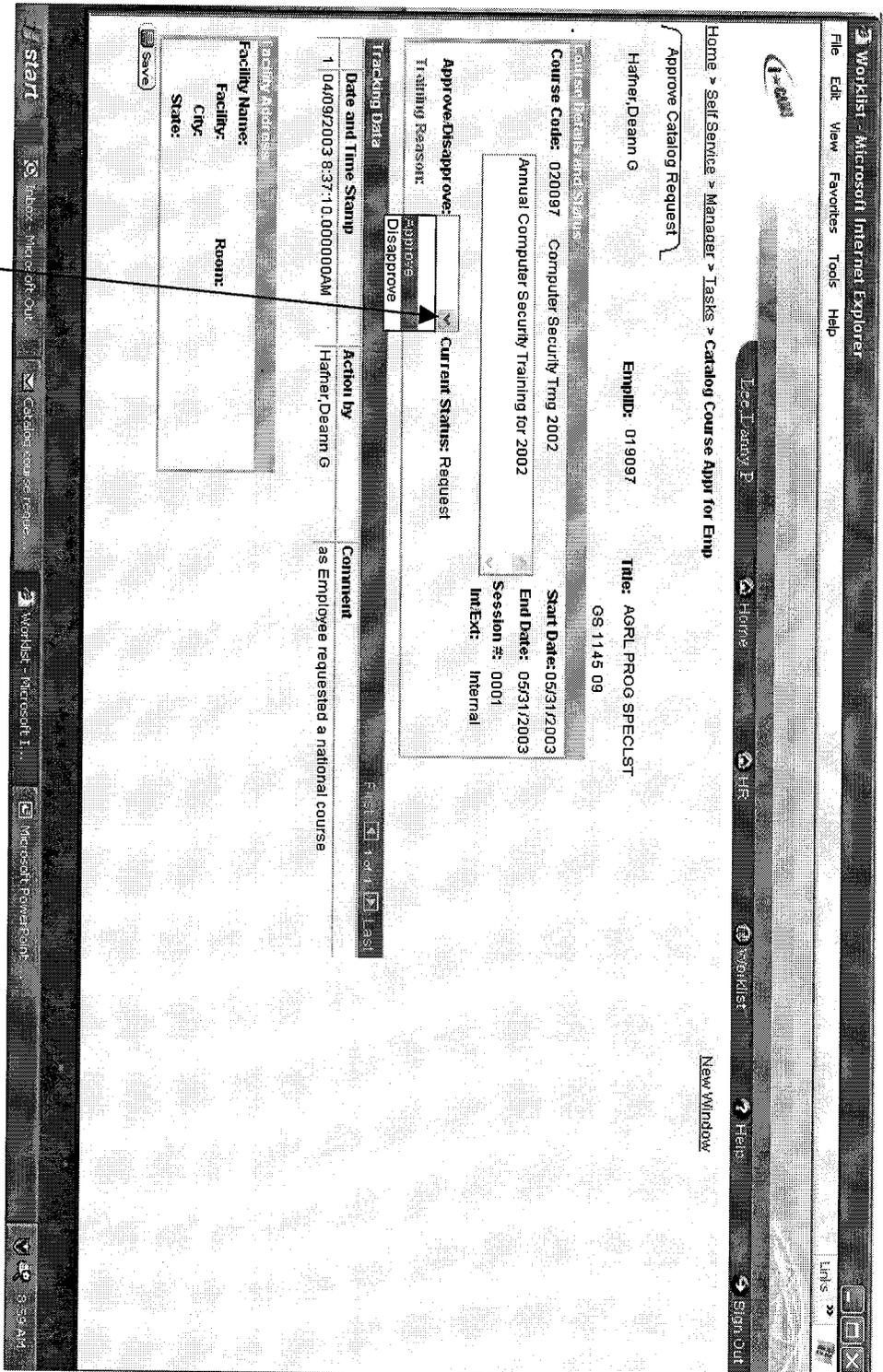
Supervisors will receive an email to notify them when employees they supervise request (certify to completion of security awareness training).



Supervisor clicks on "Worklist".

Supervisor clicks on “blue link” next to the work item “employee requested national course”.





Supervisor clicks on the drop down arrow for “current status” and makes applicable selection. The supervisor needs to verify that training has been completed by the employee before approving the training.

The screenshot shows a web application interface with the following elements:

- Navigation Menu:** Home > Self Service > Manager > Tasks > Catalog Course Applr for Emp
- Employee Information:** Employee: Halmer, Deann G (EmpID: 019097), Title: AGRL PROG SPECCLST (GS 1145 09)
- Course Details:** Course Code: 020097, Computer Security Trng 2002, Annual Computer Security Training for 2002. Start Date: 05/31/2003, End Date: 05/31/2003, Session #: 0001, IntExt: Internal.
- Approval Status:** Current Status: Request. Training Passort: Compliance.
- Tracking Data Table:**

Date and Time Stamp	Action by	Comment
1 04/09/2003 8:37:10.000000AM	Halmer, Deann G	as Employee requested a national course
- Facility Address Form:** Fields for Facility Name, City, State, and Room. A 'Save' button is located below the form.

Remember to click "Save"! The training request will flow to the HR training processor in Washington DC.

Worklist - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Home > Self Service > Manager > Tasks > Catalog Course Appr for Emp

Approve Catalog Request

Hafner, Deann G EmpID: 019097 Title: AGR1 PROG SPECCLST
OS 1145 09

Course Code: 020097 Computer Security Trng 2002 Start Date: 05/31/2003
Annual Computer Security Training for 2002 End Date: 05/31/2003
Session #: 0001
IntExt: Internal

Approve/Disapprove: APPROVE Current Status: Request Approved by Supervisor

Training Reason: Compliance

Tracking Data		
Date and Time Stamp	Action by	Comment
1 04/09/2003 8:37:10.000000AM	Hafner, Deann G	as Employee requested a national course
2 04/09/2003 9:04:28.000000AM	Lee, Danny P	as Supervisor approved the national course.

Facility Name: Room:

Facility: City: State:

Save

12 of 2 Last

Start Index - Microsoft Out... Catalog Course request... Worklist - Microsoft I... Microsoft PowerPoint

9:03 AM

Links Sign Out