

United States Department of Agriculture
Research, Education, and Economics

ARS □ NIFA □ ERS □ NASS

Bulletin

Title: Telework Security and Non-Government Furnished Equipment

Number: 13-007

Date: March 15, 2013 **Expiration:** March 16, 2014

Originating Office: Office of the Chief Information Officer, ARS

Distribution: ARS Headquarters, Areas, and Locations

This bulletin provides the ARS policy and procedures for securing non-Government Furnished Equipment used for ARS telework programs.

1 Table of Contents

1	Table of Contents	2
2	Introduction.....	334
3	Purpose.....	334
4	Policy	334
	4.1 Information Technology Equipment	334
	4.2 Non-Government Furnished Equipment (non-GFE)	334
5	Management and Operational Controls	556
	5.1 Training and Rules of Behavior	556
	5.2 Software	556
	5.3 Authentication	556
	5.4 Physical Security of Equipment and Information	556
	5.5 Freedom of Information Act and Records Management	556
	5.6 No Expectation of Privacy	667
6	Points of Contact.....	667
	6.1 Help Desk Support	667
	6.2 Incident Response	667
7	Enforcement.....	667
8	Applicable Guidance, Laws, and Regulations	778
9	Definitions.....	778
10	Abbreviations	889
	APPENDIX A: Self-Certification Security Checklist and User Telework Security Agreement Form for Non-Government Furnished Equipment	9910
	APPENDIX B: Telework Quick Start Guide.....	11112

2 Introduction

The Telework Enhancement Act of 2010 requires Federal agencies to actively expand their use of telework. ARS is committed to implementing a telework program.

On March 28, 2012, ARS published an updated telework policy, P&P 402.5 v.2, titled “The REE Telework Program.” It establishes the policy and procedures for implementing the telework initiative. This document is intended to be an interim extension of that policy that provides security guidance and procedures to allow employees to telework securely and safely.

3 Purpose

The purpose of this document is to establish interim security guidelines for personally-owned devices used to telework and to remotely access the ARS production network. This document also provides usage restrictions and implementation guidance related to non-Government Furnished Equipment (non-GFE). Finally, this document provides a user agreement for the terms and conditions as it applies to use of non-GFE.

4 Policy

Users must prevent introducing computer security vulnerabilities into ARS’ information technology systems that will weaken or compromise ARS’ security. Each user must understand his or her role and responsibility to protect the integrity of ARS’ information and reputation. Each user will not circumvent the controls that defend against or detect for threats against the integrity, availability and confidentiality of ARS’ informational resources.

4.1 Information Technology Equipment

A number of technologies may be employed to enable teleworkers to accomplish most of their regular daily duties from their alternate duty locations. ARS makes the distinction between Government Furnished Equipment (GFE) and non-Government Furnished Equipment (non-GFE). The terms “personally-owned equipment” (POE) and “non-GFE” can be used interchangeably, but for the purposes of this guidance, the term “non-GFE” will be used throughout the document. The following section provides policies for the non-GFE category.

4.2 Non-Government Furnished Equipment (non-GFE)

Non-GFE can be used for non-sensitive work and routine administrative work. Teleworkers must protect all Agency records and documents from unauthorized disclosure and damage, and must comply with all eUSDA and ARS policies. Non-GFE may be used provided that the employee adheres to the following:

- Antivirus software must be installed and kept up-to-date on the non-GFE that the teleworker uses to connect to the ARS network. The teleworker is responsible for acquiring, installing, and maintaining antivirus software for non-GFE. A full system scan is required at least once a week to check for any viruses, tracking cookies or any other malware on the computer. If the computer is shared with other members of the household, a partial virus scan for common threats must be conducted before connecting to a Federal network. There are a number of commercial vendors that offer low-cost or free antivirus services.

- When the computer is connected to the ARS network, that computer becomes part of the USDA network. Network traffic to and from the computer is continually monitored by USDA until it is disconnected. If malware (virus, Trojan, root-kit, etc.) is detected on the computer, access to USDA's network will be denied. It is the teleworker's responsibility to eradicate any malware detected on the non-GFE device.
- All operating system and software patches must be kept up-to-date on the non-GFE that the teleworker uses to connect to the ARS network. The non-GFE's operating system must be configured to allow the automatic installation of the latest software updates and security patches. Automatic updates for the operating system and applications must be enabled to check and install the updates at least once a month. If the operating system or software application is no longer supported with patch updates (e.g., Windows ME), then the owner of the non-GFE should update their computer to a more current operating system or application (e.g., Windows 7). Additionally, ARS employees may want to consult security resources that may help to determine their individual security settings on their non-GFE. For additional information, visit:
 - SecuniaPSI for patching and updating your system.
<http://secunia.com/products/consumer/psi/>
 - SANS for a few tips to help you protect your home computer.
<http://isc.sans.edu/diary.html?storyid=4849>
 - "NSA Best Practices for Home Network Security."
http://www.nsa.gov/ia/files/factsheets/Best_Practices_Datasheets.pdf
- Computers must have firewalls operating on the home network. Employees should take full advantage of the firewall usually built into the Internet Service Provider's router. Contact your Internet Service Provider for assistance. If you use Microsoft Windows, it provides a software-based firewall.
- Do not run peer-to-peer software simultaneously while actively accessing ARS systems. Examples of peer-to-peer software include Yahoo Messenger, Windows Messenger, MSN Messenger, AOL Instant Messenger, Google Talk, Bit Torrent, Edonkey, Gnutelle, Morpheus, Kazaa, Napster, and Limewire. The user will not tamper with the security controls put in place by USDA.
- No Personally Identifiable Information (PII) will be copied to any GFE or non-GFE storage devices. PII is 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, biometric records, including any other personal information that is linked or linkable to an individual.

- The teleworker must not screen capture, print or store PII or security sensitive information on a non-GFE.
- Contact your local ARS Help Desk for technical support for GFE. ARS Help Desk support for non-GFE is limited to troubleshooting installation of the ARS VPN client. See section 5.2 for a link to instructions on downloading and installing the ARS VPN client.

5 Management and Operational Controls

5.1 Training and Rules of Behavior

Users must have completed the current year's Information Security Awareness Training and understand their responsibilities for properly safeguarding Government information. Visit <http://www.aglearn.usda.gov/> for the latest Computer Security Awareness online training and search the catalog for "USDA Information Security Awareness Training." A pre-test is available if you are familiar with last year's content. It should be understood that *during duty hours, while performing official functions, there is neither expectation of, nor right to privacy on GFE or non-GFE equipment.* The performance of inappropriate activities such as viewing inappropriate Web sites, pornography or copyright violations during work hours and while connected to ARS' networks can result in disciplinary action against the employee.

5.2 Software

Teleworkers must conform to ARS software standards, including legal use of licensed software products. Files must be virus checked before they can be downloaded ~~it~~ to the ARS network. If the teleworker is using Microsoft Windows, then the teleworker must use Microsoft Internet Explorer 9 Web browser or a later version. If a non-Microsoft browser is used, the teleworker must use the latest version of that browser and the latest updates installed for that browser. VPN software and instructions on how to download the software are available at <https://arsnet.usda.gov/sites/ocio/Telework/default.aspx>.

5.3 Authentication

No LincPass cards, User IDs, passwords, PINs, and access codes are to be shared with anyone else, including coworkers, supervisors, or members of the household.

5.4 Physical Security of Equipment and Information

Teleworkers are responsible for maintaining the physical security of the equipment, work products, and software while in transit or teleworking from home. It is advisable to physically secure portable equipment with a cable lock, especially while on travel. If the employee is found negligent for the loss of equipment, the employee may be required to reimburse the Government for all costs associated with the loss of the Government-owned information. Monitors should be positioned so that they cannot be observed by unauthorized individuals.

5.5 Freedom of Information Act and Records Management

Employees with access to records that are subject to Freedom of Information Act (FOIA) and National Archives and Records Administration (NARA) Records Management regulations must maintain appropriate administrative, technical, and physical safeguards to ensure the security of

the records. Employees must adhere to all appropriate data security policies on maintaining the integrity, confidentiality, and security of Government information.

5.6 No Expectation of Privacy

All e-mail and data created, downloaded or stored on the device in connection to employee's work activity is owned by the Department of Agriculture and, for the purpose of protecting the rights and property of the Department of the Agriculture, may be monitored, intercepted, recorded, read, copied or captured and disclosed by authorized personnel for authorized purposes. There is no expectation of privacy for data that is transmitted, processed or stored during the VPN session. System personnel may be required to provide law enforcement officials any potential evidence of crime discovered on devices used for telework. *Use of personally-owned equipment to connect to the USDA network by the teleworker, authorized or unauthorized, constitutes consent to this monitoring, interception, recording, reading, copying or capturing and disclosure while connected.* It is required that the user signs the User Agreement (see Appendix A) before non-Government Furnished Equipment is used to connect to the USDA network.

6 Points of Contact

Questions about this guidance may be directed to the ARS OCIO Cybersecurity Staff at ARS-OCIO-Cybersecurity@ars.usda.gov or 301-504-4841.

6.1 Help Desk Support

Contact your local ARS Help Desk for technical support for GFE. ARS Help Desk support for non-GFE is limited to troubleshooting installation of the ARS VPN client. Help Desk support will not be available for troubleshooting hardware or software problems on non-GFE.

6.2 Incident Response

A security incident consists of a breach of security or events that indicate a security violation or attempts to gain unauthorized access to computers, information systems or data on information resources. All security incidents will be reported to ARS Cybersecurity in accordance with the ARS Incident Response Plan. Security incidents should be promptly reported to the ARS Incident Response Team at ARS-CyberIR@ars.usda.gov.

7 Enforcement

ARS will take corrective actions and/or enforce the use of penalties against any teleworker who knowingly violates any USDA, REE or Federal system security policy while connected to a USDA network. Disciplinary actions could include the following actions, up to removal:

- Written reprimands.
- Temporary suspension from duty.
- Reassignment, demotion or removal.
- Suspension of system privileges.
- Possible criminal prosecution.

8 Applicable Guidance, Laws, and Regulations

- P&P 402.5 The REE Telework Program
- P&P 253.3 ARS Cybersecurity Program
- P&P 253.4.v.2 Use of Information Technology Resources
- P&P 020 Cellular Devices and Service Management

9 Definitions

Government Furnished Equipment (GFE) [FAR 52.245-1]

Property in the possession of, or directly acquired by, the Government and subsequently furnished to the employee or contractor for performing of their duties or a contract. GFE includes, but is not limited to, spares and property furnished for repairs, maintenance, overhauling or modification. Government property means all property owned or leased by the Government. Government property includes both Government-furnished and contractor-acquired property.

Incident [NIST SP 800-61]

A violation or imminent threat of violation of computer security policies, acceptable use policies or standard security practices.

Incident Response [NIST SP 800-61]

The process of identifying, responding and reporting a security incident. Each incident is analyzed to help prevent future violations of security policies and recommended practices from recurring.

Non-Government Furnished Equipment (non-GFE)

Non-GFE is any information technology or communications equipment not acquired by the Agency or by grant money. Non-GFE is synonymous with Personally-Owned Equipment (POE), and the two terms may be used interchangeably.

Non-Sensitive Work

Any activity or communications that does not involve sensitive information.

Password Protected [NIST SP800-124]

The ability to protect the content of a file or device from being accessed until the correct password is entered.

Peer-to-Peer Software

Peer-to-peer (P2P) software enables a computer to interact with other computers for the purpose of sharing files and peripherals without the need of a central server. When computers are virtually connected together, they set up a P2P network. Each P2P network must use the same or a compatible program to connect to each other. This includes, among others: Yahoo Messenger, Windows Messenger, MSN Messenger, AOL Instant Messenger, Google Talk, Skype, Bit Torrent, Edonkey, Gnutelle, Morpheus, Kazaa, Napster, and Limeware. P2P networks can be used for sharing large audio or video files or any other large digital format. Because P2P networks use encrypted tunnels to connect computers together, it is impossible to determine if the traffic flowing through the connections is benign or if it contains malicious or illegal content.

Personally Identifiable Information (PII) [OMB M-06-19]

PII is 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.

Sensitive Information [Departmental Regulation 3440-2]

Unclassified information that, if publicly disclosed, could be expected to have a harmful impact on the security of person, place, or property. Examples include, but are not limited to, key management itineraries and schedules, Secured Compartmented Information Facilities (SCIF) Standard Operating Procedures, building vulnerabilities, guard post orders, Inspector General investigations, computer infrastructure or network details, rural development management control reviews that reveal vulnerabilities, ARS report of strategic research targets to potential American livestock and poultry from biological threat agents, Continuity of Operation relocation sites, security assessments of USDA Biosafety Level laboratories, and USDA security classification guides.

Threat [NIST SP 800-61]

The potential source of an adverse event or attack.

Vulnerability [NIST SP 800-61]

A weakness in a system, application, or network that is subject to exploitation or misuse.

10 Abbreviations

ARS	Agricultural Research Service
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
P&P	Policy and Procedures
SP	Special Publication
PII	Personally Identifiable Information
SBU/SSI	Sensitive But Unclassified/Sensitive Security Information

Paul R. Gibson
Chief Information Officer
Office of the Chief Information Officer

Date

APPENDIX A: Self-Certification Security Checklist and User Telework Security Agreement Form for Non-Government Furnished Equipment

Instructions: Use this Self-Certification Security Checklist to assess the your computer security at home.

Self-Certification Security Check List	YES	NO
1. Are your security patches, operating system and applications up-to-date? If not, access your computer’s “help and support” function and search on the keyword “update.”		
2. Do you have antivirus software installed and is it up-to-date? If using a non-GFE, you must obtain, install, and maintain your antivirus license and keep antivirus software definitions up-to-date.		
3. Is your firewall installed, active, and up-to-date? If not, or you do not know how to check, refer to your Internet Service Provider instructions.		
4. Are you using the latest version of your Web browser? If not, download the latest version, inspect for viruses, and install the browser.		

If you answered “No” to any of the questions above, please take the action noted in each category above to comply with the Self-Certification requirements.

Instructions: Eligibility will based on the employee’s Telework Agreement and will be reviewed when duties change, or when a new telework agreement is established. The supervisor is to retain the original form in the employee’s personnel files.

Section A. Signatures	
I certify that I have read and understood the arrangement described in this agreement. I further certify that I have read and understood the policy and the <i>Terms and Conditions</i> listed above, and I agree to abide by them. Failure to abide by all <i>Terms and Conditions</i> pertinent to this agreement may result in a-termination of my connectivity to ARS’ networks from my personally-owned computer or handheld wireless or mobile device, and may result in disciplinary action.	
Employee’s Signature:	Date
Supervisor’s Signature:	Date

1. Employee Name (Last, First, MI): _____

2. Organization (Agency, Division, Branch /Section): _____

Section B. Terms and Conditions

1. Non-Disclosure

I will not knowingly disclose, either during my employment or thereafter, any PII or SBU/SSI information to any person not authorized to view such information. I understand that information will only be shared on a “need-to-know” basis. I will immediately notify ARS-CyberIR@ars.usda.gov if I become aware of any unauthorized disclosure of any ARS information.

2. Privacy and Behavior

I understand that there is neither expectation of, nor right to, privacy while connected to the ARS network. I also understand that the performance of inappropriate activities such as viewing inappropriate Web sites, pornography, political activities, conducting personal business, or copyright violations while connected to USDA’s networks can result in disciplinary action. I understand that all e-mail with an ARS address and data created, downloaded, or stored in connection to my work activity is owned by the Department of Agriculture and may, for the purpose of protecting the rights and property of the Department of Agriculture, be subject to electronic discovery and records management regulations. Such e-mail and data may be monitored, intercepted, recorded, read, copied, or captured and disclosed by authorized personnel for authorized purposes.

3. Antivirus and Patch Management for Non-GFE

I understand that antivirus software must be installed on my personally-owned computer or mobile device and be kept up-to-date. I am responsible for acquiring, installing, and maintaining antivirus software for my personally-owned computer or mobile device and will run a full system scan at least once a week to check for any viruses, tracking cookies, key loggers or any other malware on the computer. I understand USDA will block access to its networks if there are any indications of intentional or unintentional security breaches that affect the overall security of the USDA network. I understand that it is my responsibility to eradicate any malware found on my personally-owned computer immediately after it is discovered. I also understand that all operating system and software patches will be kept up-to-date. I will configure my personally-owned mobile device to allow the latest software updates and security patches to be installed. I will allow automatic updates for the operating system and applications to check and install software updates at least once a month.

4. Upon Separation or When Telework Is No Longer Required for Non-GFE

I will remove all ARS distributed software from my personally-owned computer, wireless handheld or mobile device immediately upon separation from ARS, if I am no longer eligible for telework, or when the software is no longer required to perform my work. I will surrender data created while employed by ARS to my supervisor and purge it from my personally-owned computer, wireless handheld or mobile device. Exceptions may be considered if my relationship should continue with ARS as a collaborator, volunteer or contractor.

APPENDIX B: Telework Quick Start Guide

All Telework employees who intend to use non-GFE must complete the following steps:

Step	Action
1	Complete the Self-Certification Security Checklist and User Telework Security Agreement Form. The checklist and agreement can be found in Appendix A of this Bulletin (12-007).
2	Submit the following forms to your Supervisor: <ul style="list-style-type: none">• REE-45, ARS Telework Agreement (if you do not already have an approved agreement in place)• Appendix A, Bulletin 12-007, Self-Certification Security Checklist and User Telework Security Agreement Form
3	Download the AnyConnect VPN software application and installation instructions from https://arsnet.usda.gov/sites/ocio/Telework . Choose the client that is appropriate for your operating system (Windows, Mac, Linux).

Support

Contact your local ARS Help Desk for technical support for GFE. ARS Help Desk support for non-GFE is limited to troubleshooting installation of the ARS VPN client. Help Desk support will not be available for troubleshooting hardware or software problems on non-GFE.