



United States Department of Agriculture

Research, Education, and Economics
Agricultural Research Service

JUN 08 2006

SUBJECT: Unauthorized Peer-to-Peer (P2P) Programs on Government
Computers

TO: All Agency Employees

FROM: Melinda L. McClanahan
Chief Information Officer

Melinda L. McClanahan

This memo is a reminder to all ARS Employees that the use of P2P software is prohibited on all USDA equipment and networks. In accordance with Office of Management and Budget Memo 04-06 on File Sharing Technology, "Federal computer systems or networks (as well as those operated by Contractors on the government's behalf) must not be used for the downloading of illegal and/or unauthorized copyrighted content." USDA does not consider "Limited Personal Use Policy" defined in DR 3300-1 or ARS P&P 253.4 as justification for downloading P2P or other programs that perform those functions.

P2P is a protocol often used to obtain freeware, shareware, and bootleg software. P2P exchange is made practical through web sites that act as clearinghouses listing people who have or want something. Some P2P applications allow computer users to directly access files from another hard drive such as, music (mp3), movies, and documents. Other types of P2P applications include gaming, telephony, and instant messaging.

The following list gives examples of some P2P software divided by category.

Instant Messaging /Telephony

- Yahoo Messenger
- Windows Messenger
- Skype
- MSN Messenger
- AOL Instant Messenger



Office of the Chief Information Officer
5601 Sunnyside Avenue • Beltsville, MD 20705-5143
An Equal Opportunity Employer

File Sharing

- Bit Torrent
- Gnutella
- Kazaa
- WinMX
- Napster
- PC Anywhere
- Edonkey
- Morpheus
- EMule
- Limewire
- BearShare
- Timbuktu

Instant Messaging/Telephony allows users to chat via text messaging in real time in addition to sharing files and initiating telephone calls over the Internet. File Sharing and gaming allows users to search each other's hard drives for specific files or information.

P2P file sharing can potentially compromise computer systems. The use of this software creates vulnerabilities which can be exploited by providing a means of introducing malicious code and other illegal material into a Government network. In addition, the software can allow inadvertent sharing of files by vulnerabilities or misconfiguration of the software.

To enforce Department Manual 3525-002 "Internet Use & Copyright Restrictions," USDA Cyber Security is monitoring all USDA networks for P2P traffic. Upon detection of this traffic, the ARS, OCIO, Cybersecurity Branch will be notified via the Incident Handling Process.

Having this software installed and/or running on Government equipment or networks is prohibited and appropriate disciplinary action will be taken. If you currently have this type of software installed on your government equipment, it must be removed. Should you require assistance to remove this software, please contact your local help desk.

If an exception to this policy is required, please prepare and send a valid business need to include your immediate supervisor's approval and signature and email your request to ARS-OCIO-Cybersecurity@ars.usda.gov.