

Peer-to-Peer Software and Use of NRC Computers to Process SUNSI Frequently Asked Questions

1. What is peer-to-peer software?

Peer-to-peer, or P2P, file-sharing systems provide users with the ability to share files on their computers with other people through the Internet. The most popular P2P software is free and is used to share music, movies, and games, and for Instant Messaging.

2. Why is P2P a problem?

P2P software provides the capability for users to access files on other users' computers beyond those intended for sharing (i.e., music). For example, if you have P2P software on your computer and you also do your own tax preparation on your computer and store a copy of the tax return on your hard drive, other people anywhere in the world may be able to access the files containing your tax return.

3. Have sensitive government files been obtained through the use of P2P?

Yes. There are documented incidents where P2P software was used to obtain sensitive government information when peer-to-peer software was installed on a government or home computer.

4. Is someone obtaining sensitive information the only threat?

No. P2P can also make it easier for computer viruses and other malicious software to be installed on your computer without your knowledge.

5. Have other Federal agencies adopted similar policies?

Yes, other Federal agencies have adopted similar policies. The Office of Management and Budget wrote the requirements for government-wide adoption in 2004. Additionally, due to the increased awareness of the P2P threat that has arisen since 2004, DOT, DHS, DOE, DOD, and other agencies have issued specific P2P policies.

6. How do I know if peer-to-peer software is on my home computer?

If you share your home computer with other family members, you can ask them a simple question: "Do you do any type of file-sharing over the Internet?" If the answer is yes, you should ask what software is used. Some examples of commonly used P2P software are AOL Instant Messenger, Kazaa and Kazaa Lite, iMesh, Morpheus, LimeWire, Groksster, BearShare, and Gnutella. Newer P2P products include giFT, FilePipe, and Kceasy.

7. How can I identify and remove P2P software from my home computer?

P2P software can be installed as part of another product installation or it can be installed maliciously as part of spyware. It can be difficult to identify whether P2P software has been

installed on your computer, as the software can take many forms. In some instances, spyware may keep your P2P connection(s) active even though you think you have uninstalled P2P file-sharing.

There are several commercial products available to remove spyware and P2P software. None of the available products are completely effective and all of the products must be kept up-to-date by the user. Anti-spyware products have some capability to detect and/or remove P2P. A basic search on the Internet will provide many available products. For example, ZDNet provides information on P2P Doctor, software that targets and removes many P2P products. This software is not endorsed nor has it been tested by NRC staff.

8. I need P2P for my job. How do I go about getting it installed on my NRC computer?

NRC does not allow the installation and use of P2P technology without explicit written approval from the NRC Designated Approving Authority (DAA), currently the Director of the Office of Information Services. P2P software has not been authorized by the DAA. The documented vulnerabilities of P2P software, along with documented incidents of exploitation of P2P software to obtain unauthorized access to sensitive government information, require that NRC implement strict controls over P2P software. All NRC networks and systems may be monitored to identify the use of P2P software.

9. When accessing NRC e-mail from a home computer, using either NRC Webmail or broadband CITRIX, can I open attachments that contain Sensitive Unclassified Non-Safeguards Information (SUNSI)?

You can open attachments that contain SUNSI using broadband CITRIX. However, Webmail uses temporary memory on your home computer and, therefore, is readable by an outside party accessing your computer using P2P software or by someone else using your computer. Webmail should not be used to access or process SUNSI.

10. What do I do if I don't have broadband CITRIX Access?

You may request the establishment of a CITRIX broadband account by emailing your name and LAN ID to OIS_IT_Coordinator@nrc.gov.

11. Can CITRIX be installed on Macintosh computers?

Yes, but only under the following configuration:

All cryptographic modules (discrete software unit that performs mathematical operations related to encryption/decryption) that have been validated to National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) have the mode used for the validation. That mode is called "FIPS mode."

The Firefox product uses the Network Security Services (NSS) Cryptographic Module and the validation information can be found on NIST's web page at: <http://csrc.nist.gov/cryptval/140-1/140val-all.htm#815>

The security policy link from that web page can be used to obtain the security policy for the product and this policy states the following:

The NSS cryptographic module has two modes of operation: the FIPS Approved mode and non-FIPS Approved mode. By default, the module operates in the non-FIPS Approved mode. To operate the module in the FIPS Approved mode, an application must adhere to the security rules in the Security Rules section and initialize the module properly. If an application initializes the NSS cryptographic module by calling the standard PKCS #11 function `C_GetFunctionList` and calls the API functions via the function pointers in that list, it selects the non-FIPS Approved mode. To operate the NSS cryptographic module in the FIPS Approved mode, an application must call the API functions via an alternative set of function pointers. Rule 7 of the Security Rules section specifies how to do this.

12. Can the NRC accommodate a large number of employees using CITRIX at the same time?

CITRIX can currently accommodate 1,000 concurrent users, and by January 2008 it will be able to concurrently accommodate 1,200 users.

13. If I have a computer at home that cannot access the Internet, can I use that computer to create or process SUNSI?

No. While the computer may not be connected to the Internet, there are still risks that need to be addressed. Portable media you use for personal use can have malware that could infect the portable media you are using for NRC SUNSI information. That malware could then be transported to NRC's infrastructure. Additionally, when you process information on your home computer, the information is recorded in temporary storage. Other users can find the information in temporary storage on that standalone computer. The computer can also be stolen, as was the case with the Veterans Administration (VA) laptop that contained Personally Identifiable Information (PII).

14. If I have a computer at home that has broadband Internet access using fiber optic or cable modem, can I turn the modem off and then create or process SUNSI?

No. When you process information on your home computer, the information is recorded in temporary storage. P2P software can find the information in temporary storage when you turn the modem back on. Other users of your home computer can also find that information. The computer can also be stolen, as was the case with the VA laptop that contained PII.

15. If I have a computer at home that has broadband Internet access using fiber optic or cable modem, can I disconnect the cable connection and then create or process SUNSI?

No. When you process information on your home computer, the information is recorded in temporary storage. P2P software can find the information in temporary storage when you reconnect the cable. Other users of your home computer can also find that information. The computer can also be stolen, as was the case with the VA laptop that contained PII.

16. May I open an NRC e-mail (or an e-mail attachment) from my home computer, not knowing if it contains SUNSI?

You should only access NRC e-mail if it could contain SUNSI from your home computer using broadband CITRIX. If you think your e-mail could contain SUNSI, you should not access it via Webmail.

17. Can I use a wireless Internet connection to access NRC Webmail on my home computer?

No. Use of a wireless home computer connection has not been approved for remote access to NRC's LAN/WAN.

18. If I am properly logged-in to CITRIX through a dial-up phone line, may my home computer's wireless connection capability remain on?

No, your home computer's wireless connection should be off. Additionally, dial-up CITRIX is prohibited for accessing SUNSI, as it does not provide the same protections as broadband access.

19. Can I access SUNSI on my NRC-provided BlackBerry or other PDA?

You can access SUNSI on your NRC-provided BlackBerry or a personal BlackBerry that conforms to NRC's security specifications. This is because BlackBerry devices are configured to encrypt data on them and encrypt transmissions between the BlackBerry and NRC's LAN/WAN. Please note that emails sent outside NRC's LAN/WAN are not encrypted and, therefore, the content is not protected. PDAs other than BlackBerry devices have not been approved for wireless connection to NRC's LAN/WAN.

20. Are there any limitations on using an NRC-provided laptop to create or process SUNSI?

Until encryption software is available, accessing SUNSI with an NRC-provided laptop should be through broadband CITRIX. NRC is working with the General Services Administration SmartBUY program to make encryption software available to all offices. Offices will be responsible for purchasing, installing, and maintaining the encryption software.

21. Can I use a wireless connection or other non-CITRIX Internet connection to access SUNSI on an NRC-provided laptop?

Not at this time. OIS is in the process of developing a specification for wireless use of NRC-provided laptops.

22. When traveling, what are the limitations on using hotel-provided Internet access to access SUNSI from an NRC laptop?

The access must be through CITRIX broadband using a hardwire connection. Wireless connection is currently prohibited. See answer to question #21.

23. When traveling, can I access NRC e-mail or SUNSI from a hotel computer?

You can access NRC's e-mail system from a hotel computer using Webmail. You should not access SUNSI from a hotel computer. Also, see question #16.

24. When traveling, can I use a hotel computer to process SUNSI contained on a disk, CD, DVD, thumb drive, or other similar device?

No. When you process information on a hotel computer, the information is recorded in temporary storage. P2P software can find the information in temporary storage. Other users of the computer can also find that information.

25. If multiple NRC staff are traveling with only one NRC-provided laptop, can each traveler use that laptop to create SUNSI or does each traveler need their own NRC-provided laptop?

If all the travelers need to know the SUNSI information, then they can share the laptop. If there is not an equal need to know and the SUNSI information is encrypted such that only those with a need to know have access, the laptop can be shared. An example of this type of information is PII where the encryption key is not shared with other users. The users must have their own account (user ID and password) on the laptop.