POLICY ISSUE
NOTATION VOTE

September 19, 2007 SECY-07-0163

FOR: The Commissioners

FROM: Luis A. Reyes
Executive Director for Operations

SUBJECT: POLICY FOR USE OF PEER-TO-PEER SOFTWARE AND THE PEER-TO-PEER THREAT TO SENSITIVE UNCLASSIFIED NON-SAFEGUARDS INFORMATION

PURPOSE:

To provide the Commission information on the threat posed by the use of peer-to-peer (P2P) or file sharing software on U.S. Nuclear Regulatory Commission's (NRC) sensitive information and information technology infrastructure and to obtain the Commission's decision on the proposed changes to protect the information and the infrastructure.

SUMMARY:

P2P file sharing systems provide users with the ability to share files (e.g., music) on their computers with other people through the Internet. P2P software provides the capability for users to access files on other users' computers beyond those intended for sharing. There are numerous documented incidents where P2P software was exploited to obtain sensitive and classified government and commercial sector information when it was installed on government, private industry, or home computers. To limit inappropriate access to Sensitive Unclassified Non-Safeguards Information (SUNSI), the staff recommends prohibiting the installation of P2P

CONTACT: Russell Nichols, IRSD/OIS
(301) 415-6874

software on NRC computers without the explicit written approval of the NRC Designated Approving Authority (DAA), currently the Director of the Office of Information Services. In addition, to protect SUNSI from P2P exploitation via home computers, after evaluating various options, the staff recommends prohibiting downloading, storing, or processing SUNSI on home computers even when a floppy disk, CD, DVD, or thumb drive is the storage media. However, SUNSI could be processed on a home computer when the computer is connected to the NRC network via broadband CITRIX.

BACKGROUND:

On May 7, 2007, a Fox News reporter reported that he was able to use P2P software to download sensitive personal and government information from a Department of Transportation employee's home computer. The information included the employee's tax return and information considered Official Use Only that was stored on the hard drive of the employee's home computer. The reporter showed copies of the documents during the newscast.

Since July 6, 2005, the NRC has used Secure Computing's SmartFilter software to block access to Internet Web sites that are considered a potential risk to the agency. This includes sites that download software, such as P2P software, that covertly gather user information through the user's Internet connection. Use of this software significantly reduces the possibility that P2P software exists on NRC's infrastructure. However, based on recent information, the Office of Information Services has identified P2P as a potential security vulnerability when home computers connect to NRC systems or when sensitive information is downloaded, stored, or processed on home computers. The use of P2P software applications can result in the loss of sensitive information, cause damage to NRC's public image and/or to NRC systems, and use large amounts of limited bandwidth, which can adversely impact regular network operations.

P2P software provides the capability for users to access files on other users' computers beyond those intended for sharing (i.e., games and music). For example, if you have P2P software on your home computer and you also do your own tax preparation on your home 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 file containing your tax return using P2P software. 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.

According to Tiversa, a company that helps organizations and government agencies mitigate the risks associated with the inadvertent sharing of sensitive information on publicly accessible computer networks, there are more than 800 million P2P searches conducted on the Internet daily. This is more than the number of daily Google searches. There are more than 15 billion files on LimeWire alone. There are more than 450 million copies of file-sharing software and there are more than 20 million users per day using P2P software. Security experts are aware that P2P file-sharing poses a risk, but the magnitude and dimensions of the threat are surprising even the most well-informed. More than 65 percent of the Internet bandwidth is utilized daily for file-sharing activities. For a detailed explanation of the P2P threat and actions being taken by other government agencies, see Enclosure 1.

DISCUSSION:

Protection of NRC Computers

To further limit inappropriate access to SUNSI, the staff recommends prohibiting the installation of P2P software on NRC computers without the explicit written approval of the NRC DAA, currently the Director of the Office of Information Services. To date, the DAA has not approved use of P2P software on NRC's infrastructure. Prohibiting P2P software on NRC's infrastructure is consistent with what other Federal agencies are doing and with the Office of Management and Budget's guidance.

1. This recommendation would provide a high level of assurance that SUNSI would not be compromised on NRC computers because the vulnerability from P2P attack would be significantly reduced. Adding this additional level of security to NRC computers would enhance the NRC's ability to protect SUNSI from disclosure to the public and to deny it to individuals who would use it for malevolent purposes, thus contributing to public confidence in the way NRC protects sensitive information. It would also further limit the potential of NRC receiving adverse publicity because of a compromise of SUNSI as a result of file sharing via P2P software.

2. Implementation of this recommendation would require no agency-wide additional resources.

3. As part of the rules of behavior for granting access to NRC's LAN/WAN, individuals would be required to sign a document acknowledging the prohibition on installing unauthorized software and their responsibility for protecting sensitive information.

Options for Addressing Home Computers

To address the P2P vulnerability associated with home computers that are used by employees to remotely process SUNSI, the staff presents the following options.

Option 1

Prohibit the staff from downloading, storing or processing SUNSI on home computers unless connected to the NRC network via broadband CITRIX. This includes prohibiting the staff from processing SUNSI on home computers even when a floppy disk, CD, DVD, or thumb drive is the storage media.[1] Under this option, the staff who work at home would be required to perform

[1] Current policy already prohibits processing or storing personally identifiable information (PII) on a home computer and requires PII work to be done on an NRC-encrypted laptop or other encrypted mobile information device when access is from outside of the NRC LAN. In addition, current policy also prohibits working at home on confidential allegations information or saving/storing allegations information on a hard drive that is shared with others. Work at home is prohibited for Office of Investigations and Office of Inspector General information and such information may not be transmitted electronically. With regard to working at home with SUNSI, current SUNSI policy states, "To ensure that the information is not viewed or accessed inadvertently or willfully by a person not authorized access, the employee must ensure that the information cannot be seen by a family member, guest, or any other

electronic processing of SUNSI either on a home computer using the virtual environment provided by the NRC Broadband Remote Access System using CITRIX or on an NRC-issued laptop with encryption software. This policy would take effect immediately after Commission approval and notification of NRC employees of the policy change. An implementation period of three months would allow time for offices to provide laptops, where needed.

Pros

1. This option would provide a high level of assurance that SUNSI would not be compromised on home computers of NRC staff because the vulnerability from P2P attack would be significantly reduced. Adding this additional level of security to the NRC infrastructure would enhance the NRC's ability to protect SUNSI from disclosure to the public and to deny it to individuals who would use it for malevolent purposes, thus contributing to public confidence in the way NRC protects sensitive information. It would also further limit the potential of NRC receiving adverse publicity because of a compromise of SUNSI as a result of file sharing via P2P software.

2. The NRC has adequate CITRIX broadband connections. CITRIX broadband can currently accommodate 1,000 concurrent users and by October 2008 it will be able to concurrently accommodate 1,200 users.

3. Using CITRIX broadband would require no agency-wide additional resources. Any laptops needed to implement this requirement would be purchased by the offices or regions with existing funds.

4. As part of the rules of behavior for granting access to NRC's LAN/WAN, individuals would be required to sign a document acknowledging the prohibition on installing unauthorized software and their responsibility for protecting sensitive information.

5. Macintosh users with MAC OS X v10.4 or higher would be able to use CITRIX broadband by using Mozilla's Firefox v2.x web browser in the Federal Information Processing Standards mode, which can be downloaded for free from the Internet.

Cons

The staff who currently work at home on SUNSI using dial-up CITRIX access would have to obtain broadband service and obtain a CITRIX broadband service account because dial-up does not provide adequate protection against P2P vulnerabilities. Staff who would be unwilling or unable to pay the additional costs of broadband access would be de facto prohibited from working at home on SUNSI unless their office provided a laptop for work at home.

Option 2

Allow the staff to download, store, or process on their home computers without using broadband CITRIX specified classes of SUNSI that are now grouped as "sensitive internal information."

---

individual who is not authorized access."

These categories would encompass deliberative process information (advice, opinions, and recommendations) that is being developed as part of a decision-making process on a matter, attorney-client privilege, and attorney-work product. This would capture most SECY papers, rulemaking, and adjudicatory documents. This option would not allow staff to process on their home computers without use of broadband CITRIX any documents that contained proprietary information, enforcement or allegation information, security-related information, PII, or Privacy Act information. Under this option, staff would be warned that when they process "sensitive internal information" on their home computers without using broadband CITRIX there are dangers associated with P2P software use, even when a floppy disk, CD, DVD, or thumb drive is the storage media.

Pros

1. Much of the work that is currently done away from the office could be done without using broadband CITRIX.

2. Using CITRIX broadband would require no agency-wide additional resources. Any laptops needed to implement this requirement would be purchased by the offices or regions with existing funds.

Cons

Some SUNSI would be at risk because "sensitive internal information" would potentially be vulnerable to loss via P2P software.

Option 3

Warn the staff of the dangers associated with P2P software use on home computers even when a floppy disk, CD, DVD, or thumb drive is the storage media, but do not prohibit their use for processing any SUNSI except PII.

Pros

1. This option would not require the staff to use encrypted laptops for processing SUNSI, except for PII, nor would it require those who do not have broadband Internet service to obtain it.

2. This option is the most convenient option because it would require no changes to current agency policy or operations.

Cons

The same cons apply as those listed in Option 2 except that this places all SUNSI at risk, except PII, whenever SUNSI is processed on a home computer.

Option 4

Fund and implement enterprise encryption and agency-wide laptop services and support programs. This option would include all of the controls described in Option 1 but additionally would permit an agency-wide enterprise encryption program for laptops and the laptop services and support structure to maintain the encryption program.

Pros

This option is the ideal security solution because it would allow the agency to transition to and implement an enterprise architecture in which the agency uses dockable laptops that are all encrypted. This would enable the staff to take an NRC laptop home or on travel and connect to the NRC LAN in an encrypted mode, thus denying access to NRC information by unauthorized users. Laptops would be encrypted so that the data they contain could not be accessed if the laptop was lost or stolen.

Cons

This option is expensive and funding is not available in fiscal year (FY) 07 or FY 08. The funding request for enterprise encryption ($635K) in FY 08 was deferred to FY 09. However, this is $170K less than requested for FY 09. The funding for agency-wide laptop services and support (i.e., patching, upgrading, securing, etc.) in FY 08 was significantly reduced (from $1,052K to $220K) as well as in FY 09 (from $830K to $220K). The resources needed for laptop services and support were identified in the FY 08 and FY 09 budget requests as "Services and Support for SGI/Classified Workstations." Therefore, there would be a need for an additional $832K in FY 08 and an additional $610K in FY 09.

COMMITMENT:

Listed below are the actions or activities committed to by the staff in this paper:

1. After the Commission decision, the Office of the Executive Director for Operations will make appropriate notifications to the staff.

2. The SUNSI Web site will be updated, if required.

3. In addition to the information provided above, Enclosure 2 is a listing of frequently asked questions (FAQs) concerning P2P software and the use of NRC computers to process SUNSI. These FAQs will be tailored to the option approved by the Commission and posted on NRC's internal SUNSI Web site.

RECOMMENDATION:

The staff recommends P2P software be specifically prohibited on NRC infrastructure unless approved by the DAA and that Option One be approved with respect to the use of home computers.

RESOURCE:

Options 1, 2, and 3 would require no additional resources, unless offices or regions purchase their own laptops and encryption software. To implement Option 4, the FY 08 cost would be $635K for enterprise encryption and $832K for SGI/Classified workstations for a total of $1,467K. The FY 09 cost would be $170K for enterprise encryption and $610K for SGI/ Classified workstations with a total of $780K. In order to properly implement this option, the funding for the entire enterprise encryption and laptop program would need to be reinstated for FY 08 and FY 09.

COORDINATION:

The Office of the General Counsel reviewed this package and has no legal objection. The Office of the Chief Financial Officer reviewed this package for resource implications and has no objection.

/RA William F. Kane Acting For/

Luis A. Reyes
Executive Director
for Operations

Enclosures:
1. Peer-to-Peer Threat and Actions Being Taken by Other Government Agencies
2. Peer-to-Peer Software and Use of NRC Computers to Process SUNSI

Peer-to-Peer Threat and Actions Being Taken by Other Government Agencies

There are numerous documented incidents where peer-to-peer (P2P) software was exploited to obtain sensitive and classified government and commercial sector information when it was installed on government, private industry, or home computers. In June 2007, Pfizer reported that personal information of 17,000 employees was exposed through unauthorized P2P file-sharing software installed on a laptop, with 15,700 of these records subsequently accessed and copied by an unknown number of individuals.

P2P can also make it easier for computer viruses and other malicious software to be installed on your computer without your knowledge. According to the Department of Homeland Security (DHS), United States Computer Emergency Readiness Team (US-CERT), when P2P applications are used, it is difficult, if not impossible, to verify that the source of the files is trustworthy. These applications are often used by attackers to transmit malicious code. Attackers may incorporate spyware, viruses, Trojan horses, or worms into the files. When the files are downloaded, the computer becomes infected. By late spring 2005, DHS reported that government employees using file-sharing programs had repeatedly compromised national and military security by "sharing" files containing sensitive or classified data.

Another example of malicious use of P2P software includes Botnet cyber crimes. "Botnet" is derived from the idea of a "ro**bot net**work." Botnets refer to networks of computers that are able to be remotely controlled by outside sources. Using P2P software to surreptitiously access someone's computer, an attacker usually gains control by infecting the computer with a virus or other malicious code. In many instances, the computer continues to operate normally, and the owner is unaware that the computer has been compromised. Frequently, botnets are used to steal password and login data, bank account information, and other sensitive and personal data, but botnets could be used to access home computers of NRC staff to steal sensitive unclassified non-safeguards information being processed or stored on the home computer.

On July 24, 2007, the U.S. House of Representatives, Committee on Oversight and Government Reform, heard key testimony by government and industry experts who showed overwhelming agreement about the threat of inadvertent file-sharing over P2P networks. The following is an excerpt of the testimony showing some of the types of documents obtained by Tiversa.

Inadvertent shared information is not limited to classified information. A diverse amount of information exists across government agencies and contractors. Here are some examples:

- A document illustrating over 100 individual soldiers' names and Social Security numbers
- Physical threat assessments for multiple cites such as Philadelphia, St. Louis, and Miami
- A government contractor exposing an Air Force base physical security attack assessment
- A document titled "NSA Security Handbook"
- A detailed report from a well-known government contractor for the National Security Agency (NSA) which outlines how to connect two secure DoD networks

- Numerous Department of Defense Directives (DoDD's) on various Information Security topics
- Various Department of Defense Information Security system audits, reviews, procedures, etc. (e.g., retina scanner equipment audit, penetration detection software/equipment reviews)
- Numerous "Field Security Operations" documents, including router checklists procedures, "Network Infrastructure Security Checklist", etc.
- Numerous presentations for Armed Forces leadership on various Information Security topics, including how to profile "hackers" and potential internal information leakers
- Large numbers of Army documents marked "For Official Use Only"

While Congress investigates P2P, other government agencies are already taking action to protect their information from P2P software.

- The Department of Veterans Affairs has prohibited the use of P2P.

- Department of Transportation (DOT) users are not authorized to install or use P2P software applications unless expressly authorized in writing by the Department's Chief Information Officer. DOT cannot restrict P2P on personal computers; however, their policy prohibits employees from using or accessing DOT information if P2P software is installed or suspected of being installed on an employee's personal computer. The problem with this approach is that employees may not know they have P2P software installed on their computers because it can be inadvertently or unknowingly downloaded by other family members.

- DHS has updated its Rules of Behavior in the DHS Handbook to include the prohibition of P2P file-sharing or software. In addition, the DHS's proposed approach to sensitive data in telework situations is: (1) without prior approval from security, sensitive data cannot be stored on non-DHS computers; (2) staff must use Virtual Private Network from a DHS laptop only; (3) when using Outlook Web Access from a personal computer, do not open any Sensitive But Unclassified or For Official Use Only (FOUO) documents locally; (4) always secure a DHS laptop in case of theft or break in; and (5) do not print or store sensitive information at home.

- Department of Energy's (DOE) P2P Networking Guidance states, "P2P applications are not to be used on DOE systems that contain or process Sensitive Unclassified Information (SUI). The default condition is that no P2P technology or services are to be used except under conditions prescribed by Senior DOE Management in their Program Cyber Security Plans."

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.