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

[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

perform 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

---

individual who is not authorized access."

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." 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

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

ADAMS Accession No.: ML072080256 **EDATS: OIS-2007-0031**

OFFICE	QTE	IRSD/OIS	CST	ICOD	OE
NAME	L.Culp	R.Nichols	K.Lyons-Burke	T.Rich	C.Carpenter
DATE	08/03/07	08/23/07	08/29/07	08/30/07	08/30/07
OFFICE	OI	OCFO	OGC	IRSD/OIS	IRSD/OIS
NAME	M.K.Fahey	T.Croote	T.Rothschild	M.Janney	M.Thaggard
DATE	08/29/07	09/06/07	08/30/07	09/05/07	09/05/07
OFFICE	IRSD/OIS	~~DD/OIS~~	D/OIS	DEDIS/CIO	EDO
NAME	J.Linehan	~~K.Greene~~	E.Baker	D.Ash	L.Reyes
DATE	09/07/07	~~09/ /07~~	09/11/07	09/19/07	09/19/07

OFFICIAL RECORD COPY