



UNITED STATES
NUCLEAR REGULATORY COMMISSION

WASHINGTON, D.C. 20555-0001

October 18, 2007

SECRETARY

COMMISSION VOTING RECORD

DECISION ITEM: SECY-07-0163

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

The Commission (with Chairman Klein and Commissioner Lyons agreeing) approved the subject paper as recorded in the Staff Requirements Memorandum (SRM) of October 18, 2007. Commissioner Jaczko approved in part and disapproved in part.

This Record contains a summary of voting on this matter together with the individual vote sheets, views and comments of the Commission.

A handwritten signature in black ink, appearing to read "Annette L. Vietti-Cook", written over a horizontal line.

Annette L. Vietti-Cook
Secretary of the Commission

Attachments:

1. Voting Summary
2. Commissioner Vote Sheets

cc: Chairman Klein
Commissioner Jaczko
Commissioner Lyons
OGC
EDO
PDR

VOTING SUMMARY - SECY-07-0163

RECORDED VOTES

	APRVD	DISAPRVD	ABSTAIN	NOT PARTICIP	COMMENTS	DATE
CHRM. KLEIN	X					10/5/07
COMR. JACZKO	X	X			X	10/9/07
COMR. LYONS	X				X	10/2/07

COMMENT RESOLUTION

In their vote sheets, Chairman Klein and Commissioner Lyons approved the staff's recommendation and Commissioner Lyons provided some additional comments. Commissioner Jaczko approved in part and disapproved in part with comments. Subsequently, the comments of the Commission were incorporated into the guidance to staff as reflected in the SRM issued on October 18, 2007.

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary
FROM: CHAIRMAN KLEIN
SUBJECT: SECY-07-0163 – POLICY FOR USE OF PEER-TO-PEER SOFTWARE AND THE PEER-TO-PEER THREAT TO SENSITIVE UNCLASSIFIED NON-SAFEGUARDS INFORMATION

Approved xx Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below _____ Attached _____ None xx



SIGNATURE

10/5/07

DATE

Entered on "STARS" Yes No _____

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary
FROM: COMMISSIONER JACZKO
SUBJECT: SECY-07-0163 – POLICY FOR USE OF PEER-TO-PEER SOFTWARE AND THE PEER-TO-PEER THREAT TO SENSITIVE UNCLASSIFIED NON-SAFEGUARDS INFORMATION

Approved X Disapproved X Abstain

Not Participating

COMMENTS: Below Attached X None



SIGNATURE

12/9/07

DATE

Entered on "STARS" Yes X No

**Commissioner Jaczko's Comments on SECY-07-0163
Policy for Use of Peer-To-Peer Software and the Peer-To-Peer Threat
To Sensitive Unclassified Non-Safeguards Information**

I approve, in part, and disapprove, in part, the staff's recommended policy to further protect Sensitive Unclassified Non-Safeguards (SUNSI) information from potentially being compromised on NRC computers and the home computers of the agency's employees. The staff recommended that Peer-to-Peer (P2P) software be prohibited on NRC infrastructure unless approved by the Designated Approving Authority (DAA) and that agency staff be prohibited from processing SUNSI on home computers. I approve of the staff recommendation to require authorization from the DAA before allowing P2P software to be installed on NRC infrastructure. I disapprove of strictly prohibiting agency employees from processing sensitive internal information, which is one category of SUNSI, on their personal computers.

I believe that the agency must prevent computer resources and infrastructure from being compromised from potential digital security threats. While additional measures to limit inappropriate access to SUNSI should be considered, I believe it is more important to prohibit the use of P2P software on the agency's infrastructure to prevent attacks, intrusions, and even malicious code from being downloaded with P2P software which could cause damage to the infrastructure. Thus, I approve of requiring authorization from the DAA before allowing P2P software to be downloaded on agency computers. This process will allow agency managers to know exactly what software is running and keep track of the agency's software configuration.

I disapprove of the other staff recommendation because it would prohibit agency employees from being able to process, on their home computers, SUNSI now grouped under sensitive internal information. This category of SUNSI captures most SECY papers, rulemaking, and adjudicatory documents which are necessary to allow the staff the flexibility it needed to telework productively. I believe that limiting the processing of SUNSI on home computers to sensitive internal information appropriately bounds the digital risk if this information were compromised. Moreover, the agency would continue to prohibit the processing of proprietary information, enforcement or allegation information, security-related information, PII, and Privacy Act information from being processed on home computers significantly reducing the vulnerability to the inappropriate release of SUNSI. Therefore, I support Option 2, which adequately protects agency interests without impeding efficient work by employees working at home or in alternate locations.

Ultimately, I believe requiring authorization prior to the use of P2P software on agency computers and allowing agency employees the flexibility to continue to process sensitive internal information on home computers, achieves the appropriate level of security for SUNSI until the Chief Information Officer can develop an agency standard for encryption of laptops and mobile devices.



Gregory B. Jaczko

10/9/07

Date

NOTATION VOTE

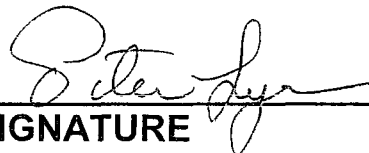
RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary
FROM: COMMISSIONER LYONS
SUBJECT: SECY-07-0163 – POLICY FOR USE OF PEER-TO-PEER SOFTWARE AND THE PEER-TO-PEER THREAT TO SENSITIVE UNCLASSIFIED NON-SAFEGUARDS INFORMATION

Approved X Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below _____ Attached X None _____



SIGNATURE

10/2/07

DATE

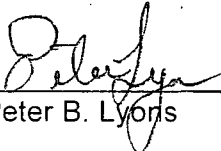
Entered on "STARS" Yes ✓ No _____

Commissioner Lyons' Comments on SECY-07-0163

I approve the staff's recommendation to prohibit the installation of P2P software on NRC computers without the explicit written approval of the NRC Designated Approving Authority in order to limit inappropriate access to SUNSI. This recommendation would limit the potential for SUNSI to be compromised on NRC computers and reduce the Agency's vulnerability to malevolent attacks via P2P software.

I approve the staff's recommendation (Option 1) to prohibit staff from working on SUNSI on a computer at home unless connected to the NRC network via broadband CITRIX or unless using an NRC-issued laptop with encryption software. Under this option, the staff could not process SUNSI on home computers even when a floppy disk, CD, DVD, or thumb drive is the storage media. The staff's recommendation has the advantage of providing a high level of assurance that SUNSI would not be compromised by P2P vulnerabilities. I recognize that this option impacts the Agency's work at home program by placing a burden on employees who use their home computers to process SUNSI material. For this reason, offices should assure that staff needing to process SUNSI at home be provided with NRC laptops if they do not have broadband CITRIX.

The option of funding enterprise encryption and agency-wide laptop services and support programs (Option 4) should be revisited as informed by the experience gained from the implementation of Option 1.


Peter B. Lyons 10/2/07
Date