October 10, 2006

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum **/RA/**
Assistant Inspector General for Audits

SUBJECT: STATUS OF RECOMMENDATIONS: EVALUATION OF PERSONAL PRIVACY INFORMATION FOUND ON NRC NETWORK DRIVES (OIG-06-A-14)

REFERENCE: DEPUTY EXECUTIVE DIRECTOR FOR INFORMATION SERVICES AND ADMINISTRATION, OFFICE OF THE EXCUTIVE DIRECTOR FOR OPERATIONS, MEMORANDUM DATED AUGUST 8, 2006

Attached is the Office of the Inspector General (OIG) analysis of recommendations as discussed in the agency's response dated August 8, 2006. Based on these responses, recommendation 1 is closed and recommendations 2, 3, and 4 are resolved. Please provide an update on the status of these recommendations by January 2, 2007.

If you have questions or concerns, please call me at 415-5915.

Attachment: As stated

cc: M. Johnson, OEDO
M. Malloy, OEDO
P. Tressler, OEDO

Audit Report

EVALUATION OF PERSONAL PRIVACY INFORMATION FOUND ON NRC NETWORK DRIVES (OIG-06-A-14)

Status of Recommendations

Recommendation 1:	Remind employees of their responsibilities to protect personal privacy information.
Response dated August 8, 2006:	Agree. All NRC employees need to be reminded of their responsibilities to protect personal privacy information. The Office of Information Services (OIS) prepared Yellow Announcement 2006-039 that reminds employees and on-site contractors of their responsibilities for safeguarding personally identifiable information. It was issued June 22, 2006.
OIG Response:	The proposed corrective action has addressed the intent of this recommendation. This recommendation is closed.
Status:	**Closed.**

Audit Report

EVALUATION OF PERSONAL PRIVACY INFORMATION FOUND ON NRC NETWORK DRIVES (OIG-06-A-14)

Status of Recommendations

Recommendation 2:	Remind employees that files on network drives may be viewed by other network users and that personal privacy information should not be posted on network drives unless access to that information is appropriately restricted to users with a "need to know."
Response dated August 8, 2006:	Agree. OIS will issue a Yellow Announcement reminding employees and on-site contractors which network drives can be accessed by other users and that personal privacy information should not be stored on these shared drives unless access to that information is appropriately restricted. This Yellow Announcement will be issued by September 30, 2006.
OIG Response:	The proposed corrective action addresses the intent of this recommendation. This recommendation will be closed when OIG verifies that the agency issues a Yellow Announcement that specifically addresses employees' ability to view and post personal privacy information on the agency network drives.
Status:	**Resolved.**

Audit Report

EVALUATION OF PERSONAL PRIVACY INFORMATION FOUND ON NRC NETWORK DRIVES (OIG-06-A-14)

Status of Recommendations

Recommendation 3:	Develop policies and procedures for reviewing network drives for the presence of personal privacy information.
Response dated August 8, 2006:	Agree. OIS will propose interim guidance regarding the agency's Sensitive Unclassified Non- Safeguards Information (SUNSI) policy to include a requirement that Office Directors and Regional Administrators ensure their staff periodically review shared network drives for personal privacy information. This guidance will ultimately be included as part of the SUNSI policy revision in response to SECY memorandum, dated June 29, 2006, entitled, "Staff Requirements — COMSECY-05-0054 — Policy Revision: Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information." The revision to the SUNSI policy will be provided to the Commission for approval in June 2007.
OIG Response:	The proposed corrective action to include this policy within the SUNSI revised policy addresses this recommendation in addition to larger issues related to sensitive information. However, the intent of this recommendation is to provide immediate guidance to NRC staff for reviewing network drives for the presence of personal privacy information which could be accomplished earlier than the proposed time frame for SUNSI policy revisions. For example, the shared drives team is developing procedures to review the network drives. Once that has been completed and this guidance is made available to the IT coordinators and other responsible parties, and OIG verifies these actions, this recommendation could be closed.
Status:	**Resolved.**

Audit Report

EVALUATION OF PERSONAL PRIVACY INFORMATION FOUND ON NRC NETWORK DRIVES (OIG-06-A-14)

Status of Recommendations

Recommendation 4:	Conduct an immediate review of all network drives for the presence of personal privacy information and remove any information that should not be posted on a network drive unless access to that information is appropriately restricted to users with a "need to know."
Response dated August 8, 2006:	Agree. In a memorandum dated June 21, 2006, Office Directors and Regional Administrators were directed to immediately begin to conduct a review of the data generated by their office or region stored on the shared drives to determine if the information is appropriate for a shared drive and either ensure access is restricted only to persons with a need to know or remove the information from the shared drive. They must report any instances in which personal privacy information generated or stored by their office was available to individuals without a need to know to OIS by September 15, 2006.
OIG Response:	The proposed corrective action addresses the intent of this recommendation. This recommendation will be closed when OIG verifies and reviews any reports from Office Directors and Regional Administrators to OIS of instances in which personal privacy information generated or stored by their office was available to individuals without a "need to know."
Status:	**Resolved.**