February 11, 2008

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) FOR FISCAL YEAR 2007 (OIG-07-A-19)

REFERENCE: DIRECTOR, OFFICE OF INFORMATION SERVICES, MEMORANDUM DATED DECEMBER 31, 2007.

Attached is the Office of the Inspector General's analysis and status of recommendations 2, 4, 5, 9, 10, and 15 as discussed in the agency's response dated December 31, 2007. From this response, recommendations 2, 9, and 10 remain resolved while recommendations 4, 5, and 15 are now closed. Previously, recommendations 1, 3, 11, 12, 13, and 14 were resolved and continue to remain resolved. Recommendations 6, 7, and 8 were previously closed. Please provide an updated status of the resolved recommendations by April 15, 2008.

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

Attachment: As stated

cc: V. Ordaz, OEDO
J. Arildsen, OEDO
P. Tressler, OEDO

Audit Report

NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2007 OIG-07-A-19

Status of Recommendations

Recommendation 2:	Categorize all NRC major applications and general support systems in accordance with FIPS 199. (This recommendation replaced recommendation #1 from OIG-A-05-A-21, which is closed)
Response Dated December 31, 2007:	The security categorization for most systems has been completed. For those systems not categorized, OIS is having discussions with the system owners on the system boundaries. Completion date: June 30, 2008.
OIG Response:	The proposed actions address the intent of the recommendation. This recommendation will be closed when OIG verifies that all major applications and support systems have completed security categorizations conducted in accordance with FIPS 199.
Status:	Resolved.

Audit Report

NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2007 OIG-07-A-19

Status of Recommendations

Recommendation 4:	For self-assessments conducted on systems without an approved security categorization, include an explanation as to how the impact levels for confidentiality, integrity, and availability were determined. This explanation should also include a discussion of any changes to the impact levels (if any) from the previous year's self-assessment. The Agency expects to complete this action by December 31, 2007.
Response Dated December 31, 2007:	This recommendation is overcome by events in that NRC will no longer perform annual self assessments. Self assessments are now part of the continuous monitoring as outlined in NIST SP-800 53A requirements. NRC is selecting core security controls to be monitored and tested annually on all MA/GSS systems. OIS recommends closing this recommendation.
OIG Response:	This recommendation is closed as the self assessments will be performed in conjunction with continuous monitoring.
Status:	Closed.

Audit Report

NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2007 OIG-07-A-19

Status of Recommendations

Recommendation 5:	Develop and implement quality assurance procedures for self-assessments.
Response Dated December 31, 2007:	This recommendation is overcome by events in that NRC will no longer perform annual self assessments. Self assessments are now part of the continuous monitoring as outlined in NIST SP-800 53A requirements. NRC is selecting core security controls to be monitored and tested annually on all MA/GSS systems. OIS recommends closing this recommendation.
OIG Response:	This recommendation is closed as the self assessments will be performed in conjunction with continuous monitoring
Status:	Closed.

Audit Report

NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2007 OIG-07-A-19

Status of Recommendations

Recommendation 9:	Complete the updates to the security categorizations of the general support systems into which the Network Continuity of Operations system components have been incorporated.
Response Dated December 31, 2007:	The updates to the security categorizations will be completed June 30, 2008.
OIG Response:	The actions taken address, in part, the intent of the recommendation. This recommendation will be closed when OIG verifies that final approval of the Security Categorization for the RAS is granted.
Status:	Resolved.

Audit Report

NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2007 OIG-07-A-19

Status of Recommendations

Recommendation 10:	Develop and implement a methodology for identifying which listed systems reside on the NRC network and which do not.
Response Dated December 31, 2008:	The methodology for identifying which systems reside on the NRC network and which do not is in place. Procedures require that as part of the system inventory, each system be identified as to whether it resides on the NRC network or not. Reporting capabilities associated with the NRC System Information Control Database system inventory resource allow for the necessary determinations in a timely way. OIS recommends closing this recommendation.
OIG Response:	The proposed actions address the intent of the recommendation. This recommendation will be closed when OIG receives documentation of the new procedures.
Status:	Resolved.

Audit Report

NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2007 OIG-07-A-19

Status of Recommendations

Recommendation 15:	Develop and implement a plan for completing the remaining e-authentication risk assessments. This plan should include the review and update of the remaining two e-authentication risk assessments originally identified in FY 2005 as having inaccuracies and inconsistencies.
Response Dated December 31, 2007:	This recommendation is overcome by events in that NRC changed the requirement to not include e-authentication risk assessments as part of the Federal Information Security Management Act process except on e-Gov systems requiring remote access. This change was noted as a change request in the NSICD change request system and incorporated into the Project management methodology and displayed on the PMM web site. OIS recommends closing this recommendation.
OIG Response:	This recommendation is closed as the e-authentications are no longer required to be completed.
Status:	Closed.