UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

November 7, 2008

MEMORANDUM TO: R. William Borchardt
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, COMPUTER SECURITY OFFICE, MEMORANDUM DATED SEPTEMBER 23, 2008

Attached is the Office of the Inspector General's analysis and status of recommendations 1, 2, 3, 10, 11, 12, 13, and 14 as discussed in the agency's response dated September 23, 2008. From this response, recommendations 1, 2, 3, 10, 12, and 13 are closed while recommendations 11 and 14 remain resolved. Recommendations 4, 5, 6, 7, 8, 9, and 15 were previously closed. Please provide an updated status of the resolved recommendations by January 30, 2009.

If you have any questions or concerns, please call me at 415-5915 or Beth Serepca, Team Leader, at 415-5911.

Attachment: As stated

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

Audit Report

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

Status of Recommendations

Recommendation 1:	Review and correct as needed all security categorizations so that they consistently reflect the information types that reside on the systems.
Response Dated September 23, 2008:	The CSO believes this recommendation has been verified by the OIG and should be closed.
OIG Response:	The proposed actions address the intent of the recommendation. OIG has verified that security categorizations are consistent with OMB Exhibit 53 submissions and have been updated to include more accurate descriptions of the information types in the system. We will continue to evaluate categorizations as part of subsequent FISMA evaluations. This recommendation is therefore closed.
Status:	Closed.

Audit Report

INDEPENDENT EVALUATION OF 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 September 23, 2008:	The CSO believes this recommendation has been verified by the OIG and should be closed.
OIG Response:	The proposed actions address the intent of the recommendation. OIG has verified that all major applications and support systems have completed security categorizations conducted in accordance with FIPS 199. This recommendation is therefore closed.
Status:	Closed.

Audit Report

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

Status of Recommendations

Recommendation 3:	Conduct annual self-assessments in accordance with current OMB and NIST guidance.
Response Dated September 23, 2008:	The CSO believes this recommendation has been verified by the OIG and should be closed.
OIG Response:	The proposed action addresses the intent of the recommendation. OIG has verified that the annual self-assessments for FY 2008 have been conducted in accordance with current OMB and NIST guidance. This recommendation is therefore closed.
Status:	Closed.

Audit Report

INDEPENDENT EVALUATION OF 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 September 23, 2008:	The CSO believes this recommendation has been addressed and should be closed.
OIG Response:	The proposed actions address the intent of the recommendation. OIG reviewed the database schema and the inventory of listed systems and agrees that the agency has developed and implemented a methodology for identifying which listed systems reside on the NRC network. This recommendation is therefore closed.
Status:	Closed.

Audit Report

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

Status of Recommendations

Recommendation 11:	Develop and implement quality assurance procedures for POA&Ms.
Response Dated September 23, 2008:	The Agency agrees with the recommendation. NRC has been working on automating the POA&M process by using NRC System Information Control Database (NSICD) to store, process, and generate the POA&Ms. Once the migration from the Excel spreadsheet to the automated process completes, NRC will draft procedures for the new process. Automating the POA&Ms process will produce a more accurate and consistent report. In addition to documenting the procedures, CSO will also prepare other procedures related to improving the quality of POA&M information. This will include: • Documentation of procedures for conducting independent verification and validation of POA&M to assure their adequacy as part of the security assessment review process. • Acquired additional contract support to assist in establishing a compliance review process in which CSO will review security documentation, conduct vulnerability scanning, and meet with each system owner on an annual basis to verify the status of remediation efforts, assess the comprehensiveness of planned corrective action, and to validate the accuracy of tasks, responsibilities, and milestones for each outstanding weakness. These activities will take place quarterly targeting approximately 25 percent of the overall number of POA&M.
OIG Response:	The proposed actions address the intent of the recommendation. This recommendation will be closed when OIG verifies that the Agency has developed and implemented quality assurance procedures for POA&Ms.
Status:	Resolved.

Audit Report

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

Status of Recommendations

Recommendation 12:	Follow NIST guidance and only issue IATOs with documentation that includes accurate identification of risks, risk mitigation plans, and security plans.
Response Dated September 23, 2008:	The CSO believes this recommendation has been verified by OIG and should be closed.
OIG Response:	The proposed action addresses the intent of the recommendation. NRC has implemented the changes in the certification and accreditation process concerning IATOs and has posted it on the PMM Website. While no new IATOs were issued after the conclusion of the FY 2007 FISMA evaluation, the agency's actions meet the intent of the recommendation. This recommendation is therefore closed.
Status:	Closed.

Audit Report

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

Status of Recommendations

Recommendation 13:	Develop and implement quality assurance procedures to ensure certification and accreditation documentation is consistent with NIST guidance.
Response Dated September 23, 2008:	The CSO believes this recommendation has been verified by the OIG and should be closed.
OIG Response:	The proposed actions address the intent of the recommendation. OIG has verified that the Agency has developed and implemented quality assurance procedures to ensure all certification and accreditation documentation is consistent with NIST guidance. This recommendation is therefore closed.
Status:	Closed.

Audit Report

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

Status of Recommendations

Recommendation 14:	Develop and implement procedures for ensuring employees and contractors with significant IT security responsibilities are identified, receive security awareness and training, and the individual and associated training are readily identifiable.
Response Dated September 23, 2008:	All NRC offices have provided their identification of individuals with significant IT security responsibilities to the CSO. The CSO will request updates to the identification on an annual basis. The CSO provided system administrators with a Microsoft Windows server security course, and 14 staff attended the course. CSO also provided system owner training to system owners in August and September 2008. 54% of system owners attended the course. The course will be added to the iLearn system to enable others to take the course. CSO is developing a role-based training plan and expects to have the plan completed by the end of the first quarter FY09.
OIG Response:	The proposed action addresses the intent of the recommendation. OIG will close this recommendation after OIG verifies that the agency has developed and implemented procedures for ensuring all employees and contractors with significant IT responsibilities are identified and have received the needed training.
Status:	Resolved.