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

OFFICE OF THE
INSPECTOR GENERAL

April 16, 2009

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 FY 2007 (OIG-07-A-19)

REFERENCE: DIRECTOR, COMPUTER SECURITY OFFICE, MEMORANDUM DATED MARCH 24, 2009

Attached is the Office of the Inspector General's analysis and status of recommendations 11 and 14 as discussed in the agency's response dated March 24, 2009. From this response, recommendations 11 and 14 remain resolved. Recommendations 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, and 15 were previously closed. Please provide an updated status of the resolved recommendations by June 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 11:	Develop and implement quality assurance procedures for Plan of Action and Milestones (POA&Ms).
Agency Response Dated March 24, 2009:	The Agency agrees with the recommendation. CSO has been working on automating the Plan of Action and Milestones (POA&M) process and is currently analyzing a variety of tools to support this effort. NRC has draft procedures to ensure quality assurance is emphasized. The draft procedures include documentation of a process for conducting independent verification and validation of POA&M to assure their adequacy as part of the security assessment review process. Additionally, CSO has 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&Ms. Implementation of this process is scheduled for the third quarter of FY 09.
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 14:	Develop and implement procedures for ensuring employees and contractors with significant IT security responsibilities are identified, receive security awareness training, and the individuals and associated training are readily identifiable.
Agency Response Dated March 24, 2009:	The CSO provided system administrators and ISSO with Defense in Depth, Microsoft Framework Essentials (MOF), MOF 4.0 Managing Change/Configuration/Risk, System Administrator Awareness, and ISSO Awareness courses. CSO is developing 2 additional role-based training courses for ISSO/System administrator course plan and expects to have the plan completed by the end of the first quarter FY 09.
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.