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

OFFICE OF THE
INSPECTOR GENERAL

October 30, 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 OCTOBER 9, 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 October 9, 2009. Based on this response, recommendation 11 remains resolved. Recommendation 14 is closed. 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 recommendation by March 31, 2010.

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: N. Mamish , OEDO
J. Andersen, OEDO
J. Arildsen, OEDO
C. Jaegers, OEDO

Audit Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) 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 October 9, 2009:	After six months of research and evaluation the CSO picked Xacta as the agency's tool for automating the Plan of Action and Milestones (POA&M). CSO recently purchased Xacta application. Additionally, CSO developed POA&M process (ML092810195) and planned to start meeting with the system owners in the first quarter of FY10.
OIG Response:	The proposed actions address the intent of the OIG's recommendation. This recommendation will be closed when OIG verifies that agency has developed and implemented quality assurance procedures for managing POA&M.
Status:	Resolved.

Audit Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) 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 October 9, 2009:	All IT security roles were identified via a datacall issued 7/13/09 by CSO to all offices. The IT Security Role-Based Training Plan, available at: http://www.internal.nrc.gov/CSO/documents/FINAL%20IT%20Role-Based%20Training%20Plan.doc, states the requirement for training for those with significant IT responsibilities, the type of training expected for each role, and frequency of training per role. CSO is working with a contractor to draft and present 6 specific role-based courses which address 6 roles (ISSO, System Administrator, IT Manager/System Owner, and Executive/Sr. Manager). There are 2 ISSO courses planned second quarter FY10, the Sr. Manager/Executive course and the IT Manager/System Owner course planned for third quarter FY10, and 2 System Administrator courses anticipated for first quarter FY11. The System Owner is responsible for using the training plan procedures to address the training needs of his/her personnel with IT roles. This recommendation should be closed.
OIG Response:	OIG's contractor reviewed the procedures and determined that the agency identified all staff with significant IT security responsibilities by issuing data calls in April and July 2008. The agency also developed an IT Role-Based Training plan that states the requirement for training for those with significant IT responsibilities, the type of training expected for each role, and frequency of training per role. System owners are responsible for using the training plan procedures to address the training needs of his/her personnel with IT roles. The training plan defines the various

Audit Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) FOR FISCAL YEAR 2007

(OIG-07-A-19)

Status of Recommendations

Recommendation 14 (continued):

IT security roles with significant IT security responsibilities that require role-based training. NRC is pursuing three approaches to address IT role-based training: NRC-provided resident courses, use of Information System Security Line of Business providers, and commercially provided training and certifications. This recommendation is therefore considered closed.

Status: Closed