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

OFFICE OF THE
INSPECTOR GENERAL

May 6, 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 APRIL 14, 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 April 14, 2008. From this response, these recommendations remain resolved while recommendations 4, 5, 6, 7, 8, 9, and 15 were closed previously. Please provide an updated status of the resolved recommendations by September 26, 2008.

If you have any questions or concerns, please call me at 415-5915 or Beth Serepca 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 April 14, 2008:	The agency has started the process of reviewing and correcting security categorization. The IG's recommendation is now part of the agency's security categorization process by reviewing current line of business or service type, sub-function or service component, and any other related mission types. Computer Security Office (CSO) anticipates completion of review and correction security categorizations by September 30, 2008.
OIG Response:	The proposed actions address the intent of the recommendation. This recommendation will be closed when OIG verifies that all security categorizations are consistent with OMB Exhibit 53 submissions and are updated to include more accurate descriptions of the information types in the system.
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 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 April 14, 2008:	The agency has completed categorization of approximately 57% of all major applications and general support systems. Computer Security Office (CSO) anticipates completion of the remaining systems by 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

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 April 14, 2008:	The agency anticipates system owners will perform self assessments on only those systems that had not undergone certification and accreditation during previous twelve months. Self assessments will conform to NIST 800-53A. The CSO are working on refining the controls list to limit the number of controls that have to be tested annually. Due to resource constraint, system owners now anticipate date for full compliance is August 15, 2008
OIG Response:	The proposed action addresses the intent of the recommendation. This recommendation will be closed once OIG verifies that the annual self assessments for FY 2008 have been conducted in accordance with current OMB and NIST guidance.
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 10:	Develop and implement a methodology for identifying which listed systems reside on the NRC network and which do not.
Response Dated April 14, 2008:	The agency continues to update system inventory database reporting tool to reflect which listed systems reside on the NRC network and which do not. OIS is working with system owners on procedure to ensure system database reflects changes in a timely and efficient fashion. Currently, 85% of our systems in inventory reflect correct system-type. NRC is also working on restructuring its database to make reporting and data entry more efficient. Due resource constraints and required change needed to restructure database, the agency expects to complete this action by June 30, 2008.
OIG Response:	The proposed actions address the intent of the recommendation. This recommendation will be closed when OIG receives documentation that the systems are correct and that a methodology has been developed.
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 11:	Develop and implement quality assurance procedures for POA&Ms.
Response Dated April 14, 2008:	The agency has acquired the use of EPA's ASSERT tool to further automated POA&M process and continuous monitoring. OIS estimate starting implementation of NRC systems data into ASSERT tool May 1, 2008. CSO has started development of a plan to ensure QA is included in the POA&M process. The plan includes: • The development of a POA&M checklist • The use of contract to perform Independent Verification and Validation • Quarterly review of system and program level 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 April 14, 2008:	NRC has implemented the change in the C&A process and has posted relevant accreditation decision process information on the PMM web site. he agency's new Designated Approving Authority (DAA) makes decision based on the results of the security certification package, which provides the DAA with the essential information needed to make a credible, risk-based decision for **Authorization to operate, Interim authorization to operate or Denial of authorization to operate** information systems. All systems with IATO will be revisited to ensure new procedure is followed before the issuing of IATO.
OIG Response:	The proposed action addresses the intent of the recommendation. This recommendation will be closed when OIG verifies that the agency has revisited all with IATOs to ensure that the new procedure is being followed.
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 13:	Develop and implement quality assurance procedures to ensure certification and accreditation documentation is consistent with NIST guidance.
Response Dated April 14, 2008:	NRC is in the process of developing evaluation criteria checklist for three additional documents. The agency will continue to develop evaluation checklist and distribute to all system owners and certifying agents. NRC is currently soliciting feedback from certifying agents and System Owners on checklist developed so far. NRC also plans to use contract support for reviewing and providing feedback on documents and packages to system owners.
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 to ensure all certification and accreditation documentation is consistent with NIST guidance.
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 and training, and the individual and associated training are readily identifiable.
Response Dated April 14, 2008:	Memorandum sent to Office Directors and Regional Administrators on April 3, 2008 requesting identification of personnel with significant information technology security responsibilities.
OIG Response:	The proposed action addresses the intent of the recommendation. OIG will close this recommendation when OIG verifies that the Agency has developed and implemented procedures for ensuring employees and contractors with significant IT responsibilities are identified and have received the needed training.
Status:	Resolved.