September 23, 2005

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2004 (OIG-04-A-22)

REFERENCE: DIRECTOR, OFFICE OF INFORMATION SERVICES MEMORANDUM DATED AUGUST 30, 2005

Attached is the Office of the Inspector General's analysis and status of the resolved recommendations as discussed in the agency's response dated August 30, 2005. Recommendations, 2, 3, 5, 6, 7, 8, 9, and 10, remain resolved. Recommendations 1, 4, 11, 12, 13, 14, 15 and 16 have been closed. Please provide an updated status of the resolved recommendations by January 30, 2006.

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

Attachment: As stated

cc: W. Dean, OEDO
M. Malloy, OEDO
P. Tressler, OEDO

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2004
OIG-04-A-22

Status of Recommendations

Recommendation 2:	Update the Security Services Agreement (SSA) between the Department of the Interior National Business Center and NRC to include a requirement to exchange relevant system security plans.
Response Dated August 30, 2005:	**Status:** The agreement was signed on December 23, 2004. Language to exchange security plans will be addressed and included in the Interconnect Security Agreement (ISA) (See recommendation 3). DOI/NBC does not include this language in the SSA for any of their customers. A copy of the signed SSA is attached for your information. We will provide a copy of the ISA after all signatures have been obtained. DOI/NBC has provided OIS a copy of the DOI Federal Financial Systems (FFS) Security Plan dated September 2004, which is stored in the OIS security document repository located at T6 D1 and is available for IG review.
OIG Response:	The proposed corrective action addresses the intent of this recommendation. This recommendation will be closed when OIG receives and evaluates the updated Security Services Agreement. The copy of the signed Security Services Agreement has not been updated to include a requirement to exchange relevant system security plans.
Status:	Resolved.

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2004
OIG-04-A-22

Status of Recommendations

Recommendation 3:	Develop a Service Level Agreement (SLA) and Interconnect Security Agreement (ISA) between the Department of the Interior National Business Center and NRC as described in the DOI Evaluation Report, "Review of Information System Security Over Systems and Applications Used by the National Business Center to Provide Services to Non-Department of the Interior Clients."
Response Dated August 30, 2005:	**Status:** The ISA has not been signed. A revised draft version prepared by the NRC has been sent to DOI for review. The ISA version sent from DOI did not specifically address the requirement that language for exchanging security plans be included. The OIG memo of April 27, 2005, contains the requirement to include language requiring the exchange of relevant system security plans. OIS will work with the DOI point of contact to determine where this language can best be incorporated into the ISA.
OIG Response:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives and evaluates the updated Security Services Agreement and Interconnect Security Agreement.
Status:	Resolved.

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2004
OIG-04-A-22

Status of Recommendations

Recommendation 5:	Re-certify and re-accredit the NRC Data Center/Telecommunications System.
Response Dated August 30, 2005:	**Status:** The Data Center and Telecommunications (DC/T) Risk Assessment submitted March 1, 2005, was not accepted. The Commission paper on Security Program provided a new schedule for full Certification and Accreditation (C&A) by November 30, 2005. Interim Authority to Operate the DC/T was issued on July 27, 2005, to operate through November 30, 2005.
OIG Response:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives and evaluates the approved re-accreditation letter.
Status:	Resolved.

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2004
OIG-04-A-22

Status of Recommendations

Recommendation 6:	Re-certify and re-accredit the NRC Local Area Network/Wide Area Network (LAN/WAN).
Response Dated August 30, 2005:	**Status:** The LAN/WAN became very large and complex and as a result, full system certification was almost impossible. As a result, the LAN/WAN has been broken into smaller logical components that constitute several discrete "general support", "listed", and "other" systems. The re-certification and re-accreditation of the redefined LAN/WAN will be delayed until June 30, 2006. The LAN/WAN has an interim authority to operate (IATO) which expires on June 30, 2006.
OIG Response:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives and evaluates the approved accreditation letter for the redefined LAN/WAN.
Status:	Resolved.

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2004
OIG-04-A-22

Status of Recommendations

Recommendation 7:	Re-certify and re-accredit the Emergency Response Data System (ERDS).
Response Dated August 30, 2005:	**Status:** NSIR Incident Response Directorate staff, in conjunction with staff from the Office of Information Services, Program Management, Policy Development, and Analysis Staff, are pursuing a re-evaluation of ERDS and the Emergency Telecommunications System (ETS) to determine appropriate security categorization. Once stakeholder consensus is reached in regard to categorization, certification and accreditation will be pursued. Full accreditation expires on October 8, 2005.
OIG Response:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives and evaluates the approved accreditation letter.
Status:	Resolved.

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2004
OIG-04-A-22

Status of Recommendations

Recommendation 8:	Re-certify and re-accredit the Emergency Telecommunications System (ETS).
Response Dated August 30, 2005:	**Status:** NSIR Incident Response Directorate staff, in conjunction with staff from the Office of Information Services, Program Management, Policy Development, and Analysis Staff, are pursuing a re-evaluation of ERDS and ETS to determine appropriate security categorization. Once stakeholder consensus is reached in regard to categorization, certification and accreditation will be pursued. Full accreditation expires on October 8, 2005.
OIG Response:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives and evaluates the approved ETS accreditation letter.
Status:	Resolved.

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2004
OIG-04-A-22

Status of Recommendations

Recommendation 9:	Update the NRC Local Area Network/Wide Area Network (LAN/WAN) Risk Assessment.
Response Dated August 30, 2005:	**Status:** The scope of the LAN/WAN has been redefined. The Risk Assessment is estimated to be complete by April 11, 2006. See Recommendation 6 Status for more detail.
OIG Response:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives and evaluates the updated LAN/WAN Risk Assessment.
Status:	Resolved.

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2004
OIG-04-A-22

Status of Recommendations

Recommendation 10:	Update the NRC Local Area Network/Wide Area Network (LAN/WAN) Business Continuity Plan.
Response Dated August 30, 2005:	**Status:** The scope of the LAN/WAN has been redefined and the Business Continuity Plan will be complete by June 19, 2006. See Recommendation 6 Status for more detail.
OIG Response:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives and evaluates the updated LAN/WAN Business Continuity Plan.
Status:	Resolved.