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

OFFICE OF THE
INSPECTOR GENERAL

December 3, 2009

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: INFORMATION SYSTEM SECURITY EVALUATION OF REGION II - ATLANTA, GA (OIG-09-A-13)

REFERENCE: DEPUTY EXECUTIVE DIRECTOR FOR REACTOR AND PREPAREDNESS PROGRAMS, OFFICE OF THE EXECUTIVE DIRECTOR FOR OPERATIONS, MEMORANDUM DATED OCTOBER 28, 2009

Attached is the Office of the Inspector General's analysis and status of recommendations 1-10, as discussed in the agency's response dated October 28, 2009. Based on this response, all recommendations are resolved. Please provide an updated status of the resolved recommendations by June 30, 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. Arlidsen, OEDO
C. Jaegers, OEDO

Audit Report

INFORMATION SYSTEM SECURITY EVALUATION OF REGION II – ATLANTA, GA

OIG-09-A-13

Status of Recommendations

Recommendation 1:	Document key management procedures.
Agency Response Dated October 28, 2009:	Agree. Region II will document the key management procedures. This document will provide step-by-step procedures for the entire key management process, including (i) instructions for issuing and collecting keys, (ii) instructions for reporting lost or stolen keys, (iii) instructions for conducting semi-annual key inventories, (iv) the circumstances under which CyberLocks should be re-programmed, (v) the location of extra CyberKeys and the key inventory, (vi) instructions for programming the CyberKeys and the CyberLocks and (vii) the location of key management documentation. Anticipated completion date: August 4, 2010.
OIG Analysis:	The proposed corrective action meets the intent of this recommendation. This recommendation will be closed when OIG receives a copy of the key management procedures.
Status:	Resolved.

Audit Report

INFORMATION SYSTEM SECURITY EVALUATION OF REGION II – ATLANTA, GA

OIG-09-A-13

Status of Recommendations

Recommendation 2:	Include the date combinations were last changed in the combination inventory.
Agency Response Dated October 28, 2009:	Agree. The Combination Inventory shall be updated to include a field which lists the date the combination was last changed and a field which indicates the date that the combination is due to be changed. Combinations shall be changed at least annually. Anticipated completion date: August 4, 2010.
OIG Analysis:	The proposed corrective action meets the intent of this recommendation. This recommendation will be closed when OIG receives a copy of the inventory and determines that it includes the fields listing when the locks were last changed and the next due date for the combination change.
Status:	Resolved.

Audit Report

INFORMATION SYSTEM SECURITY EVALUATION OF REGION II – ATLANTA, GA

OIG-09-A-13

Status of Recommendations

Recommendation 3:	Document combination management procedures.
Agency Response Dated October 28, 2009:	Agree. Region II will document the combination management procedures. This document will provide step-by-step procedures for the entire combination management process, including (i) the circumstances under which combinations should be changed, (ii) the instructions for changing combinations and (iii) the location of combination management documentation. Combinations shall be changed at least annually. Anticipated completion date: August 4, 2010.
OIG Analysis:	The proposed corrective action meets the intent of this recommendation. This recommendation will be closed when OIG receives a copy of the combination management procedures.
Status:	Resolved.

Audit Report

INFORMATION SYSTEM SECURITY EVALUATION OF REGION II – ATLANTA, GA

OIG-09-A-13

Status of Recommendations

Recommendation 4:	Update documented backup procedures to reflect the actual backup procedures in place.
Agency Response Dated October 28, 2009:	Agree. Region II will document the actual backup procedures in place. This document will provide step-by-step procedures for the current backup process, including (i) the backup schedule, which outlines the type of backup to be performed for each day of the week and the retention period of the backup, (ii) full backups are to be performed at least weekly, (iii) full backups are to be supplemented by incremental or differential backups depending upon the scheme selected, (iv) a minimum of two (2) full backups shall be maintained - the most current shall be stored on-site, the other shall be removed to an off-site storage facility, (v) the storage location of each backup job - backups should be stored in a waterproof/fireproof safe or an approved off-site storage facility, (vi) the retrieval process for all backups stored off-site, and (vii) the procedures needed to restore data from the backup. Backups should be periodically tested, not exceed six (6) months between tests, to ensure that they can be used to effectively restore data. Anticipated completion date: August 4, 2010.
OIG Analysis:	The proposed corrective action meets the intent of this recommendation. This recommendation will be closed when OIG receives a copy of the updated backup procedures.
Status:	Resolved.

Audit Report

INFORMATION SYSTEM SECURITY EVALUATION OF REGION II – ATLANTA, GA

OIG-09-A-13

Status of Recommendations

Recommendation 5:	Develop and implement procedures for sending information system backup information to an offsite location for storage for at least 14 days or as recommended by the agency. The offsite storage location should be in a cabinet or safe that is waterproof and fireproof.
Agency Response Dated October 28, 2009:	Agree: Region II has implemented an off-site storage contract for system backup information. As of August 10, 2009, Region II has been storing backups off-site. Completion date: August 10, 2009.
OIG Analysis:	The proposed corrective action addresses the intent of this recommendation. This recommendation will be closed when the agency provides documentation of the procedures specifying that the offsite storage location is a cabinet or safe that is waterproof and fireproof.
Status:	Resolved.

Audit Report

INFORMATION SYSTEM SECURITY EVALUATION OF REGION II – ATLANTA, GA

OIG-09-A-13

Status of Recommendations

Recommendation 6:	Develop and document a contingency plan for the Region II seat-managed infrastructure servers.
Agency Response Dated October 28, 2009:	Agree. Region II will work with Office of Information Services (OIS) to include the Region II seat-managed infrastructure servers in the NRC's information technology infrastructure (ITI) contingency plan. Anticipated completion date: August 4, 2010.
OIG Analysis:	The proposed corrective action addresses the intent of this recommendation. This recommendation will be closed when OIG receives a copy of the contingency plan for seat-managed infrastructure servers.
Status:	Resolved.

Audit Report

INFORMATION SYSTEM SECURITY EVALUATION OF REGION II – ATLANTA, GA

OIG-09-A-13

Status of Recommendations

Recommendation 7:	Develop and document a contingency plan for the Region II NRC-managed servers.
Agency Response Dated October 28, 2009:	Agree. Region II will work with OIS to include the Region II NRC-managed servers in the NRC's information technology infrastructure (ITI) contingency plan. Anticipated completion date: August 4, 2010.
OIG Analysis:	The proposed corrective action addresses the intent of this recommendation. This recommendation will be closed when OIG receives a copy of the contingency plan for NRC-managed servers.
Status:	Resolved.

Audit Report

INFORMATION SYSTEM SECURITY EVALUATION OF REGION II – ATLANTA, GA

OIG-09-A-13

Status of Recommendations

Recommendation 8:	Develop and document a contingency plan for the Region II badge access system servers.
Agency Response Dated October 28, 2009:	Agree. Region II will work with OIS to include the Region II badge access servers in the NRC's information technology infrastructure (ITI) contingency plan. Anticipated completion date: August 4, 2010.
OIG Analysis:	The proposed corrective action addresses the intent of this recommendation. This recommendation will be closed when OIG receives a copy of the contingency plan for the badge access system servers.
Status:	Resolved.

Audit Report

INFORMATION SYSTEM SECURITY EVALUATION OF REGION II – ATLANTA, GA

OIG-09-A-13

Status of Recommendations

Recommendation 9:	Evaluate the vulnerabilities identified by the network vulnerability assessment and develop a plan and schedule to identify any false positives and to resolve the remaining vulnerabilities.
Agency Response Dated October 28, 2009:	Agree. Region II will work with the Computer Security Office (CSO) and OIS to evaluate the vulnerabilities identified by the network vulnerability assessment and develop a plan and schedule to identify any false positives and resolve remaining vulnerabilities. Anticipated completion date: August 4, 2010.
OIG Analysis:	The proposed corrective action addresses the intent of this recommendation. This recommendation will be closed when OIG receives a copy of the plan to identify any false positive and also resolve any remaining vulnerabilities.
Status:	Resolved.

Audit Report

INFORMATION SYSTEM SECURITY EVALUATION OF REGION II – ATLANTA, GA

OIG-09-A-13

Status of Recommendations

Recommendation 10	Perform a network vulnerability scan following remediation to verify all vulnerabilities have been resolved.
Agency Response Dated October 28, 2009:	Agree. Region II will work with the CSO and OIS to perform subsequent network vulnerability scan following remediation to verify all vulnerabilities have been resolved. Anticipated completion date: August 4, 2010.
OIG Analysis:	The proposed corrective action addresses the intent of this recommendation. This recommendation will be closed when OIG receives a copy of the network scan verifying that all vulnerabilities have been resolved.
Status:	Resolved.