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

OFFICE OF THE
INSPECTOR GENERAL

December 20, 2012

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 FOR FISCAL YEAR 2012 (OIG-13-A-03)

REFERENCE: DEPUTY EXECUTIVE DIRECTOR FOR CORPORATE MANAGEMENT MEMORANDUM DATED DECEMBER 7, 2012

Attached is the Office of the Inspector General's (OIG) analysis and status of the recommendations as discussed in the agency's response dated December 7, 2012. Based on this response, recommendations 1 – 13 are resolved. Please provide an updated status of the resolved recommendations by July 12, 2013.

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
K. Brock, OEDO
J. Arildsen, OEDO
C. Jaegers, OEDO

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012
OIG-13-A-03

Status of Recommendations

Recommendation 1:	Update all procedures, guides, and user manuals that provide guidance for maintaining system inventory records within NSICD [Nuclear Regulatory Commission System Information Control Database] to clearly define which organizations(s) are responsible for adding new system inventory records in NSICD.
Agency Response Dated December 7, 2012:	Agree. The Office of Information Services (OIS) has two procedures prepared and in review that reiterate the responsibilities for entering new system information in NSICD. These will be reviewed and issued prior to the next Federal Information Security Management Act (FISMA) audit. Basically, there is no change in responsibilities from today; they will just be reiterated for "new systems."
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives a copy of the procedures and determines that the procedures clearly define which organizations are responsible for adding new system records in NSICD.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012
OIG-13-A-03

Status of Recommendations

Recommendation 2:	Update the instructions included with the biannual inventory update to require system owners to notify the agency of any new systems that are not reflected in the data call.
Agency Response Dated December 7, 2012:	Agree. This will also be accomplished by the updated procedures mentioned in Recommendation 1. The requirement to notify OIS of any new systems was implied in the previous procedure. In the revised procedures, it is directly specified. **Completion Date**: March 30, 2013 **Point of Contact**: Neil Forehand, OIS
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives a copy of the procedures and determines that the procedures require system owners to notify the agency of any new systems that are not reflected in the data call.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012
OIG-13-A-03

Status of Recommendations

Recommendation 3:	Include all systems in NSICD, including all independent standalone hardware that has an NSICD system inventory number, in future biannual inventory update data calls.
Agency Response Dated December 7, 2012:	Agree. OIS recognizes that there is a need to clarify inventory by system numbers. However, OIS does not want to have inventory repeated in multiple systems. OIS will work with the Office of Administration (ADM) and the Computer Security Office (CSO) to look at current inventory tracking systems and to define a method by which inventory can be clearly associated with and reported on by a system inventory number. **Completion Date**: June 30, 2013 **Point of Contact**: Neil Forehand, OIS
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG has verified that NRC has chosen a method by which inventory can be clearly associated with, and reported on, by a system inventory number.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012 OIG-13-A-03

Status of Recommendations

Recommendation 4:	Assign responsibility for ensuring each NRC remote location maintains a consolidated inventory of all the IT system components located in that location, associated rack diagrams are kept up-to-date, and the inventory meets NRC requirements.
Agency Response Dated December 7, 2012:	Agree. All parties agree that these responsibilities should be clear. In Fiscal Year (FY) 2013, 2nd Quarter, OIS will work with each NRC remote location to discuss these responsibilities. **Completion Date**: March 30, 2013 **Point of Contact**: David Offutt, OIS
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG has verification that the responsibility was assigned for ensuring each NRC remote location maintains a consolidated inventory of all the IT system components located in that location, associated rack diagrams are kept up-to-date, and the inventory meets NRC requirements.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012
OIG-13-A-03

Status of Recommendations

Recommendation 5:	Create a consolidated inventory that meets NRC requirements of all the IT system components located in each NRC remote location.
Agency Response Dated December 7, 2012:	Agree. OIS recognizes that there is a need to be able to easily identify system components located in each NRC remote location. However, OIS does not want to have inventory repeated in multiple systems. OIS will work with ADM, CSO, and remote locations to look at current inventory tracking systems and to define a method by which inventory can be clearly and easily associated with and reported by location. **Completion Date**: June 30, 2013 **Point of Contact**: David Offutt, OIS
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that a method was selected by which inventory can be clearly and easily associated with and reported by location.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012 OIG-13-A-03

Status of Recommendations

Recommendation 6:	Update the rack diagrams for each NRC remote location.
Agency Response Dated December 7, 2012:	Agree. OIS will work with NRC remote locations to define responsibilities and the process for updating remote location rack diagrams. **Completion Date**: June 30, 2013, OIS **Point of Contact**: David Offutt, OIS
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the rack diagrams have been updated.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012 OIG-13-A-03

Status of Recommendations

Recommendation 7:	Provide refresher training to all staff responsible for implementing NRC's POA&M process.
Agency Response Dated December 7, 2012:	Agree. CSO will provide refresher training to staff responsible for implementing NRC's POA&M process. **Completion Date**: September 30, 2013 **Point of Contact**: Paul Ricketts, CSO
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the refresher training has been provided.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012 OIG-13-A-03

Status of Recommendations

Recommendation 8:	Configure the agency's automated POA&M tool to do the following: (i) prevent scheduled completion dates from being changed, (ii) prevent weaknesses from being created without a scheduled completion date or weakness source, (iii) prevent weaknesses from being closed without specifying an actual date closed, (iv) prevent users from entering actual completion dates in the future, (v) prevent users from entering an actual completion date when the status is not closed, and (vi) automatically change the weakness status from on track to delayed once the scheduled completion date has passed.
Agency Response Dated December 7, 2012:	Agree. CSO will work to identify the resources required to address the modifications outlined in the OIG's recommendation and, pending resource availability, will reconfigure the automated POA&M tool. CSO plans to coordinate its efforts with offices responsible for managing POA&Ms. **Completion Date**: September 30, 2013 **Point of Contact**: Paul Ricketts, CSO
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the agency's automated POA&M tool has been configured as discussed in the recommendation.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012 OIG-13-A-03

Status of Recommendations

Recommendation 9:	Update the IT environment contingency plan to include procedures for responding to short-term disruptions (those that last less than 24 hours), such as restoring components using alternate equipment or performing some or all of the affected business processes using alternate processing (manual) means.
Agency Response Dated December 7, 2012:	Agree. OIS will update the appropriate system contingency plans. **Completion Date**: September 30, 2013 **Point of Contact**: David Offutt, OIS
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the IT environment contingency plan has been updated to include procedures for responding to short-term disruptions.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012
OIG-13-A-03

Status of Recommendations

Recommendation 10:	Update the IT environment contingency plan to update contingency planning procedures specific to NRC remote locations that are not up-to-date. Specifically, update the list of IT environment servers supporting NRC remote locations that are referenced in Appendix H of the IT environment contingency plan and update the contingency plans for NRC remote locations that are attached to the IT environment contingency plan.
Agency Response Dated December 7, 2012:	Agree. OIS will update the appropriate system contingency plans. **Completion Date**: September 30, 2013 **Point of Contact**: David Offutt, OIS
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that OIS has updated the appropriate system contingency plans.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012
OIG-13-A-03

Status of Recommendations

Recommendation 11:	Update the IT environment contingency plan to include contingency procedures for the IT environment and other IT components supporting the one NRC remote location for which these procedures are missing.
Agency Response Dated December 7, 2012:	Agree. OIS will update the appropriate contingency procedures for any remote location that is not currently listed. **Completion Date**: September 30, 2013 **Point of Contact**: David Offutt, OIS
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that OIS has updated the IT environment contingency plan to include contingency procedures for the IT environment and other IT components supporting the one NRC remote location for which these procedures are missing.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012
OIG-13-A-03

Status of Recommendations

Recommendation 12:	Update the COOPs for NRC remote locations that are referenced in Appendix G of the IT environment contingency plan to include current IT environment configurations at NRC remote locations and to address situations where the IT environment at those locations is unavailable for any reason.
Agency Response Dated December 7, 2012:	Agree. OIS will update the contingency plan appendix. **Completion Date**: September 30, 2013 **Point of Contact**: David Offutt, OIS
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that OIS updated the COOPs for NRC remote locations that are referenced in Appendix G of the IT environment contingency plan to include current IT environment configurations at NRC remote locations and to address situations where the IT environment at those locations is unavailable for any reason.
Status:	Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012
OIG-13-A-03

Status of Recommendations

Recommendation 13:	Develop a COOP for the IT environment and other IT components supporting the one NRC remote location that does not have a COOP.
Agency Response Dated December 7, 2012:	Agree. OIS will work with any remote location that does not have a COOP plan to develop one. **Completion Date**: September 30, 2013 **Point of Contact**: David Offutt, OIS
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that OIS has developed a COOP for the IT environment and other IT components supporting the one NRC remote location that does not have a COOP.
Status:	Resolved.