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

OFFICE OF THE
INSPECTOR GENERAL

August 15, 2013

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 JULY 19, 2013

Attached is the Office of the Inspector General's (OIG) analysis and status of the recommendations as discussed in the agency's response dated July 19, 2013. Based on this response, recommendations 1, 2, 3, and 4 are closed and recommendations 5 – 13 remain in resolved status. Please provide an updated status of the resolved recommendations by October 31, 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: R. Mitchell, 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 July 19, 2013: Guidance for the NSICD data call and update process currently includes the following two procedures and the Report Instruction Guide provided for each data call. The annual "System Inventory Report Instruction Guide" is updated and presented to respondents for each data call, and is available for the balance of the year on the Data Call Reference SharePoint Site. The User Guide previously referenced in procedure 0001 R1 is no longer maintained or used in connection with the maintenance of system inventory records in NSCID. (The reference to this User Guide has been removed from Procedure OIS-9000D-0001 R1.)

1) Procedure OIS-9000D-0001, "Automated Information System (AIS) Inventory Update Data Collection Procedure," Rev.1 has been updated as follows:

    a) Para 6.1, #3 adds responsibility to notify System Owners in the data call instructions to identify new systems.
    b) Para 6.2, #6 states that all changes to data reported by systems owners are input to NSICD by the OIS Enterprise Architecture (EA) Team.

2) Procedure OIS-9000D-0002, "Entering New Records and Updating System Inventory (SI) Data in the U.S. Nuclear Regulatory Commission (NRC) System Information Control Database (NSICD)," Rev. 1 has been updated as follows:

    a) Para 5.4.1, #3 further specifies that new systems are input to NSICD by the "Maintainer" which is further defined in Para 5.5 as EA Team members.

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 (cont.):

	Target Completion Date: OIS recommends closing this recommendation.
OIG Analysis:	OIG reviewed the attachments and determined that the procedures, guides and user manuals that provide guidance have all been updated as needed to fulfill the requirements of the recommendation. This recommendation is therefore considered closed.
Status:	Closed.

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 July 19, 2013:	OIS has updated the guidance for the NSICD data call and update process to address OIG Recommendation 2, as follows: 1) In Procedure OIS-9000D-0001 R1, Para 6.2, #3 addresses the system owner's responsibility to identify new systems that have not been included in the inventory list. 2) In the "2013 System Inventory Report Instruction Guide," the Note associated with Page 2, Section A.1 states the requirement for the respondent to add new systems. Target Completion Date: OIS recommends closing this recommendation.
OIG Analysis:	OIG reviewed the attachment and determined that the guidance has been updated as needed to fulfill the requirement of the recommendation. This recommendation is therefore considered closed.
Status:	Closed.

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 July 19, 2013:	To address OIG Recommendation 3, OIS has updated Section B, page 12, of the "2013 System Inventory Report Instruction Guide" to discuss the responsibility to update all independent standalone systems with inventory numbers, in accordance with the spreadsheet in their office reference folders. (Offices that have had these assets in the past have a spreadsheet identifying them in their current office reference folders.) Note: The offices have indicated that most of these assets will be excessed in the near future. Target Completion Date: OIS recommends closing this recommendation.
OIG Analysis:	OIG reviewed the attachment and determined that the updated "2013 System Inventory Report Instruction Guide" includes all systems in NSICD for the future biannual inventory update data calls. This recommendation is therefore considered closed.
Status:	Closed.

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 July 19, 2013:	The NRC has an Information Technology Infrastructure (ITI) Information System Security Officer (ISSO), who is responsible for maintaining the IT system inventory and associated rack diagrams for items included within the ITI system boundary. The NRC also has an assigned ISSO at each of the remote locations to assist the ITI ISSO in maintaining the ITI inventory and rack diagrams. The ISSOs at the remote locations are also responsible for maintaining IT system inventory and rack diagrams for components that are not part of the ITI system boundary. Target Completion Date: OIS recommends closing this recommendation.
OIG Analysis:	OIG has verified that NRC has assigned responsibility for each NRC remote location to an ISSO to maintain a consolidated inventory of all the IT system components located in that location, keep associated rack diagrams up-to-date, and ensure that the inventory meets NRC requirements. This recommendation is therefore considered closed.
Status:	Closed.

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 July 19, 2013:	OIS identified a method for tracking inventory across HQ and remote locations by June 30, 2013. OIS has now initiated the development of the consolidated inventory and projects that this work will require fifteen months for completion. OIS has selected the technology for an inventory tracking system, and is currently defining a method to ensure that the inventory can be clearly and easily associated with and reported by location. In addition, OIS has initiated the development of the inventory system to include all IT system components for Headquarters (HQ) and each of the NRC's remote locations. We anticipate that this will take an additional 15 months. Current Target Completion Date: September 30, 2014
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 July 19, 2013:	The target date for this recommendation has changed as a result of competing priorities and resource constraints. Rack diagrams for each remote location exist and are maintained by the ISSO at each remote location. OIS will work with the ISSOs from each remote location to verify that the rack diagrams have been updated. Current Target Completion Date: September 30, 2013
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 July 19, 2013:	POA&M training/briefing materials are in draft form and undergoing internal review. Upon CSO approval of these materials, we will begin scheduling training sessions during the 4th Quarter of FY 2013. The target completion date remains valid. Target Completion Date: September 30, 2013
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 July 19, 2013:	CSO has coordinated with the vendor to implement these configuration recommendations. Our analysis determined that these items do not work as designed, and vendor modifications are required as a result of the functionality of the current POA&M tool. The NRC submitted change requests to the vendor to address the identified modifications. The vendor has developed a new version of the POA&M tool, which is currently under evaluation and testing in the Centralized Testing Facility (CTF). In accordance with the POA&M tool release notes, Recommendations 8(iv) and 8(v) have been implemented in this version. CSO will continue coordination and testing efforts with the vendor to resolve all identified limitations, and then proceed with implementing the remaining recommendations. Current Target Completion Date: September 30, 2014
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 July 19, 2013:	OIS is on track to update the ITI system contingency plan to include procedures for responding to short-term disruptions. Completion Date: September 30, 2013
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 July 19, 2013:	OIS is on track to update the ITI system contingency plan to include procedures specific to NRC remote locations that are not up-to-date. Target Completion Date: September 30, 2013
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 July 19, 2013:	OIS is on track to update the ITI system contingency plan to include COOPs for NRC remote locations that are referenced in Appendix G 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.
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 July 19, 2013:	OIS is on track to develop a COOP for the one NRC remote location that does not have a COOP. Target Completion Date: September 30, 2013
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 July 19, 2013:	OIS is on track to develop a COOP for the one NRC remote location that does not have a COOP. Target Completion Date: September 30, 2013
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that OIS 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.