



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

**OFFICE OF THE  
INSPECTOR GENERAL**

January 14, 2014

MEMORANDUM TO: Mark A. Satorius  
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 2013 (OIG-14-A-03)

REFERENCE: DEPUTY EXECUTIVE DIRECTOR FOR CORPORATE  
MANAGEMENT MEMORANDUM DATED DECEMBER 19,  
2013

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated December 19, 2013. Based on this response, recommendations 1, 2, and 3 are resolved. Please provide an updated status of the resolved recommendations by January 2, 2015.

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  
M. Khanna, 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 2013

OIG-14-A-03

#### Status of Recommendations

Recommendation 1:

Update the information in the NRC inventory for contractor systems to include missing information and to correctly classify contractor systems in accordance with CSO-PROS-2030, NRC Risk Management Framework.

Agency Response Dated  
December 19, 2013:

Agree. The Computer Security Office (CSO) will formulate a plan of action to correct the inventory discrepancies related to cybersecurity fields, develop an inventory update process and procedure for the cybersecurity fields, and develop a tasking for contract support staff to update and maintain the cybersecurity fields of the inventory.

The Office of Information Services (OIS) will work with CSO to formulate a plan of action to ensure that all NRC systems, including contractor systems, are included in the inventory. OIS will request System Owners provide updated system information in the next inventory data call.

Completion Date: December 31, 2014

OIG Analysis:

The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives documentation that the inventory includes all systems, including contractor systems, and that the contractor systems are correctly classified.

Status:

Resolved.

## Evaluation Report

### INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2013

OIG-14-A-03

#### Status of Recommendations

<u>Recommendation 2:</u>	Based on the updated inventory of contractor systems, identify those that are not compliant with CSO-PROS-2030, NRC Risk Management Framework, and complete appropriate authorization activities for those systems.
Agency Response Dated December 19, 2013:	Agree. CSO is developing processes and oversight methods to ensure the system owners of contractor systems are compliant with CSO-PROS-2030, NRC Risk Management Framework, and will complete the appropriate authorization activities for those systems.  Completion Date: December 31, 2014
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives documentation that the updated inventory of contractor systems has identified the systems not in compliance with CSO-PROS-2030, NRC Risk Management Framework, and the appropriate authorization activities for those systems have been completed.
Status:	Resolved.

## Evaluation Report

### INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2013

OIG-14-A-03

#### Status of Recommendations

Recommendation 3: Develop procedures for ensuring the annual IT security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.

Agency Response Dated  
December 19, 2013:

Agree. CSO is developing processes and oversight methods to ensure the annual IT security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.

Completion Date: December 31, 2014

OIG Analysis:

The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives documentation of the procedures for ensuring the annual IT security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.

Status:

Resolved.