



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

**OFFICE OF THE
INSPECTOR GENERAL**

April 23, 2015

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: DIRECTOR, COMPUTER SECURITY OFFICE,
MEMORANDUM DATED FEBRUARY 23, 2015

Attached is the Office of the Inspector General's analysis and status of recommendations as discussed in the agency's response dated February 23, 2015. Based on this response, recommendations 1, 2, and 3 remain resolved. Please provide an updated status of the resolved recommendations by July 31, 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: T. Rich, CSO
M. Galloway, OEDO
B. Pham, OEDO
J. Arildsen, OEDO
EDO_ACS Distribution Resource

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
February 23, 2015:

CSO formulated an approach to correct the inventory discrepancies related to computer security fields, and tasked support staff to update and maintain the computer security fields of the inventory. In conjunction with OIS, CSO worked to ensure that all NRC systems are included in the inventory. During FY2014, substantial progress was made in reducing errors, increasing the accuracy of inventory data, and updating the CSO inventory user guide. FY2015 efforts will include increased standardization of inventory nomenclature and continue to improve the accuracy and completeness of the data.

Target Completion Date: December 31, 2015

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

Recommendation 2: 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
February 23, 2015:

Agree. In calendar year 2014, testing of all systems categorized as contractor systems was completed, and authorization of these systems will be completed by the third quarter of FY2015. The next update of the annual risk management activities guidance is planned to include the explicit requirement that all contractor systems be authorized as per NRC policy.

Target Completion Date: June 30, 2015

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
February 23, 2015:

The next updates of the NRC Information Security Continuous Monitoring Process (CSO-PROS-1323) and annual risk management activities guidance are planned to include the explicit requirement that all contractor systems be authorized as per NRC policy.

Target Completion Date: December 31, 2015

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.