



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

**OFFICE OF THE  
INSPECTOR GENERAL**

July 7, 2010

**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 U.S. NUCLEAR REGULATORY  
COMMISSION'S IMPLEMENTATION OF THE FEDERAL  
INFORMATION SECURITY MANAGEMENT ACT FOR  
FISCAL YEAR 2008 (OIG-08-A-18)

**REFERENCE:** DIRECTOR, COMPUTER SECURITY OFFICE,  
MEMORANDUM DATED JUNE 11, 2010

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated June 11, 2010. Based on this response, recommendations 1 and 2 are now closed and recommendation 4 remains in resolved status. Recommendation 3 was closed previously. Please provide an update on recommendation 4 by December 1, 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. Arildsen, OEDO  
C. Jaegers, OEDO

## Audit Report

# INDEPENDENT EVALUATION OF U.S. NUCLEAR REGULATORY COMMISSION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

OIG-08-A-18

### Status of Recommendations

Recommendation 1: Update the NRC System Information Control Database to identify all interfaces between systems.

Agency Response Dated  
June 11, 2010:

CSO has completed updating interface information in NSICD with the most recent (FY09 or later) System Security Plans (SSPs) available in ADAMS. The latest inventory was submitted to OIG FISMA auditors on 5/26/2010 for review. The list of SSPs used to verify interface information can be made available upon request. CSO recommends that this item be closed.

OIG Analysis:

The OIG FISMA auditor reviewed the NRC System Information Control Database and determined that all interfaces between systems were identified. This recommendation is therefore considered closed.

**Status:**

Closed.

## Audit Report

# INDEPENDENT EVALUATION OF U.S. NUCLEAR REGULATORY COMMISSION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

OIG-08-A-18

### Status of Recommendations

Recommendation 2: Develop and implement procedures to ensure interface information in the NRC System Information Control Database is consistent with interface information in security plans and risk assessments.

Agency Response Dated  
June 11, 2010:

Entering Data into the NSICD Security Record has been updated with the following: "A list of system interfaces can be found in the system security plan. CSO staff must verify and update the interface information in NSICD using the interface information from the updated system security plans submitted by System Owners to CSO by June 15<sup>th</sup> of every year. Verification and update of the interface information in NSICD must be completed within 30 days of receiving the annual system security plan updates. CSO staff must follow up with the System Owner to resolve any inconsistencies and ensure interface information is contained in the system security plan rather than reference other documents." Additionally, we have also included requirements for reviewing system interfaces as part of our continuous monitoring program. Please see Section 2.3, Table 3-1 pg. 14, and Table 3-9 pg. 20 of Continuous Monitoring Program document (ML101530477). CSO recommends that this item be closed.

OIG Analysis: OIG reviewed the Continuous Monitoring Program document and determined that procedures were developed and implemented. This recommendation is therefore considered closed.

**Status:** Closed.

## Audit Report

# INDEPENDENT EVALUATION OF U.S. NUCLEAR REGULATORY COMMISSION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

OIG-08-A-18

### Status of Recommendations

Recommendation 4: Develop a process for verifying that all Federal Desktop Core Configuration controls are implemented for all desktop and laptop computers, including both those that are centrally managed under the agency's seat management contract and those that are owned by the agency regardless of whether or not they are connected to the agency's network.

Agency Response Dated  
June 11, 2010:

CSO will use the Secure Content Automation Protocol (SCAP) and FDCC compliance auditing tools to verify that the agency is compliant with M-08-22 for both OIS centrally managed and Region / Program Office managed computer assets. CSO will run the NIST approved scanning tools against the Agency's image for standalone computers and against the agencies General Support Systems and Major Applications during system certification and accreditation and throughout continuous monitoring and quarterly security scanning, as required by FISMA. The SCAP and FDCC compliance tools will be part of the CSO Information Assurance System (IAS), which is scheduled to be deployed early Fiscal Year 2011.

OIG Analysis: The proposed action addresses the intent of this recommendation. This recommendation will be closed when OIG verifies that the agency has completed the CSO Information Assurance System, which is necessary for NRC to provide agencywide real-time FDCC assessments.

**Status:** Resolved.