



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

OFFICE OF THE
INSPECTOR GENERAL

April 15, 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 NRC'S IMPLEMENTATION OF THE
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
FOR FISCAL YEAR 2008 (OIG-08-A-18)

REFERENCE: DIRECTOR, COMPUTER SECURITY OFFICE,
MEMORANDUM DATED MARCH 30, 2010

Attached is the Office of the Inspector General's analysis and status of recommendations 1, 2, and 4 as discussed in the agency's response dated March 30, 2010. Based on this response, recommendations 1, 2, and 4 remain in resolved status. Recommendation 3 was closed previously. Please provide an updated status of the resolved recommendations by June 15, 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. Arlidsen, OEDO
C. Jaegers, OEDO

Audit Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

OIG-08-A-18

Status of Recommendations

Recommendation 1: Update the U.S. Nuclear Regulatory Commission (NRC) System Information Control Database to identify all interfaces between systems.

Agency Response Dated
March 30, 2010:

CSO is in the process of verifying and updating the interface information in NSICD against System Security Plans that are official agency records in ADAMS. Estimated Completion Date: May 15, 2010. The results of ongoing CSO continuous monitoring reviews of NRC Offices will also be used to update this information throughout FY10.

OIG Analysis: The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives documentation that the agency identified all interfaces between systems.

Status: Resolved.

Audit Report

INDEPENDENT EVALUATION OF NRC'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
March 30, 2010:

CSO is in the process of updating the Administrative Guide for Entering Data into the NSICD Security Record to direct CSO staff to verify and update the interface information from the updated SSPs submitted by System Owners to CSO by June 15th of every year. The guide specifies that the interface information in NSICD must be verified and updated 30 days of the annual SSP update submission. The guide will direct CSO staff to follow up with the System Owner to resolve any inconsistencies and ensure interface information is contained in the SSP and not recorded as a pointer to other documents such as the Risk Assessment or the Security Categorization. CSO has also updated the continuous monitoring process to include criteria to evaluate System Owner actions to update system interface information annually during the annual continuous monitoring reviews of each office and their respective systems. Estimated Completion Date: May 15, 2010.

OIG Analysis: The proposed action meets the intent of the recommendation. This recommendation will remain resolved until the OIG verifies that the procedures developed to ensure interface information in NSICD are consistent with interface information in security plans and risk assessments are further refined.

Status: Resolved.

Audit Report

INDEPENDENT EVALUATION OF NRC'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
March 30, 2010:

The NRC has deployed the Security Content Automation Protocol (SCAP) scanners to verify that the agency is compliant with M-08-22, "Guidance on the Federal Desktop Core Configuration (FDCC)" during the system certification and accreditation process. The CSO is currently in the process of constructing its Information Assurance System (IAS) which will further enhance and complement NRC's ability to create a disposition of real-time, IT Security situational awareness. Adherence to FDCC guidelines to ensure compliance of networked computers as part of CSO's continuing monitoring assurance activities is part of an already instituted IT Security practice. Standalone systems are configured to FDCC standards during computer build-out. CSO actions regarding this particular recommendation are nearing completion. The IAS is scheduled to begin production deployment in September 2010, and is considered a core capability in the NRC's mission to provide agency wide, real-time FDCC assessments.

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 IAS which is necessary for NRC to provide agencywide real-time FDCC assessments.

Status: Resolved.