



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

**OFFICE OF THE
INSPECTOR GENERAL**

February 11, 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 2011 (OIG-12-A-04)

REFERENCE: DIRECTOR, COMPUTER SECURITY OFFICE,
MEMORANDUM DATED JANUARY 31, 2014

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations 1 through 6 as discussed in the agency's response dated January 31, 2014. Based on this response, recommendations 2 and 3 are closed and recommendations 1, 4, 5, and 6 remain resolved. Please provide an updated status on the resolved recommendations by July 31, 2014.

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 2011

OIG-12-A-04

Status of Recommendations

Recommendation 1: Develop and implement an organizationwide risk management strategy that is consistent with NIST SP 800-37 and NIST SP 800-39.

Agency Response Dated
January 31, 2014:

The Enterprise Risk Management Project Plan was published October 25, 2013, and is posted on the Computer Security Office (CSO), Computer Security Issuances, Computer Security Plans web page. The agency continues its efforts to implement an organization-wide risk management strategy that is consistent with the National Institutes of Standards and Technology (NIST) Standard Procedure (SP) 800-37 and NIST SP 800-39.

Target Completion date: December 30, 2014, pending availability of funds

OIG Analysis: The proposed corrective action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the risk management strategy has been implemented.

Status: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2011

OIG-12-A-04

Status of Recommendations

Recommendation 2: Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure standard baseline configurations are implemented for all systems.

Agency Response Dated
January 31, 2014:

The following activities support the recommendation that the baseline configurations for all systems be documented.

- NRC issued Management Directive (MD) 12.5, "NRC Cyber Security Program," on August 15, 2013. It provided specific guidance for establishing configuration management requirements, processes and procedures.
- The Standards Working Group (SWG) continues its efforts to convert standards into templates. Microsoft Windows 2007 has been completed. The SWG and the Automated Compliance Team (ACT), which is comprised of CSO staff, Office of Information Services (OIS) staff, and contractors, are working to complete the automated template for Microsoft Windows 2008, R2.
- OIS has a configuration management tool in place with a validated scanning template for one widely used operating system. A second operating system template is currently being validated and a schedule is being set for developing and validating additional templates.

The tasks needed to sufficiently address this recommendation have been completed, and this item should be considered closed.

OIG Analysis: OIG's contractor reviewed the actions taken and determined that the actions were sufficient to close 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 2011

OIG-12-A-04

Status of Recommendations

Recommendation 3: Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure baseline configurations are documented for all systems.

Agency Response Dated
January 31, 2014:

- NRC issued MD 12.5, "NRC Cyber Security Program," on August 15, 2013. It provided specific guidance for establishing configuration management requirements, processes and procedures.
- The SWG continues its efforts to convert standards into templates. Microsoft Windows 2007 has been completed. The SWG and the ACT are working to complete the automated template for Microsoft Windows 2008, R2.
- OIS has a configuration management tool in place with a validated scanning template for one widely used operating system. A second operating system template is currently being validated and a schedule is being set for developing and validating additional templates. The tasks needed to sufficiently address this recommendation have been completed, and this item should be considered closed.

OIG Analysis: OIG's contractor reviewed the actions taken and determined the actions were sufficient to close this 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 2011

OIG-12-A-04

Status of Recommendations

Recommendation 4: Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure software compliance assessments, including vulnerability assessments, are performed as required: (i) before a system is connected to the NRC production environment, (ii) during security test and evaluation of systems, and (iii) as part of the agency's continuous monitoring environment.

Agency Response Dated
January 31, 2014:

OIS has a configuration management tool in place with a validated scanning template for one widely used operating system. A second operating system template is currently being validated and a schedule is being set for developing and validating additional templates.

Completion date: June 30, 2014, pending availability of funds

OIG Analysis:

The proposed corrective actions meet the intent of the recommendation. This recommendation will be closed when OIG receives verification that the configuration management procedures have been modified accordingly.

Status:

Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2011

OIG-12-A-04

Status of Recommendations

Recommendation 5: Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure all systems components are included in requisite software compliance assessments.

Agency Response Dated
January 31, 2014:

OIS has a configuration management tool in place with a validated scanning template for one widely used operating system. A second operating system template is currently being validated and a schedule is being set for developing and validating additional templates.

Completion date: June 30, 2014, pending availability of funds

OIG Analysis: The proposed corrective actions meet the intent of the recommendation. This recommendation will be closed when OIG receives verification that the configuration management procedures have been modified accordingly.

Status: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2011

OIG-12-A-04

Status of Recommendations

Recommendation 6: Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure all identified vulnerabilities, including configuration-related vulnerabilities, scan findings and security patch-related vulnerabilities, are remediated in a timely manner in accordance with the timeframes established by NRC.

Agency Response Dated
January 31, 2014:

OIS has a configuration management tool in place with a validated scanning template for one widely used operating system. A second operating system template is currently being validated and a schedule is being set for developing and validating additional templates.

Completion date: June 30, 2014, pending availability of funds

OIG Analysis: The proposed corrective actions meet the intent of the recommendation. This recommendation will be closed when OIG receives verification that the configuration management procedures have been modified accordingly.

Status: Resolved.