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

OFFICE OF THE
INSPECTOR GENERAL

May 23, 2013

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 2011 (OIG-12-A-04)

REFERENCE: DIRECTOR, COMPUTER SECURITY OFFICE, MEMORANDUM DATED MAY 1, 2013

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 May 1, 2013. Based on this response, recommendations 1 through 6 are resolved. Please provide an update on all recommendations by January 30, 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
J. Arildsen, OEDO
K. Brock, OEDO
C. Jaegers, OEDO

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 May 1, 2013:	The agency developed and approved an Enterprise Wide Risk Management Plan. The agency proposes amending the target completion date from December 30, 2013, to December 30, 2014. 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.

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 May 1, 2013: The following activities support the recommendation that the baseline configurations for all systems be documented.

- Management Directive (MD) 12.5, NRC Automated Information Security Program, is due to be released by September 30, 2013, and will provide updated Nuclear Regulatory Commission (NRC) specific guidance for establishing configuration management requirements, processes and procedures.

- CSO established the Standards Working Group (SWG), which consists of participants from NRC offices who are stakeholders in the development of configuration baseline standards. The SWG is in the process of developing several configuration standards for existing and future technologies. As standards are developed and approved; they are, where possible, converted into templates that can be used by the agency's configuration management scanning tool. The use of the tool provides the capability to automate the configuration monitoring of assets in the agency's production environment.

- The Office of Information Services (OIS) currently has a configuration monitoring tool in place.

- The NRC is participating as an early adopter in the Continuous Diagnostics and Mitigation (CDM) program being offered by the Department of Homeland Security. The objective of the CDM program is to establish a government-wide contract to obtain tools and services that will provide Federal agencies as well as state and local governments with the ability to enhance and automate their existing continuous network

Recommendation 2 (cont.):

monitoring capabilities, correlate and analyze critical security-related information, and strengthen risk-based decision making at the agency and federal enterprise level. Information obtained from the automated monitoring tools will allow for the correlation and analysis of security-related information across the federal enterprise. The goal of NRC's participation in the CDM program is to leverage the provided tools and services to gain assistance in maturing the agency's system inventory, vulnerability and configuration management capabilities.

Target Completion date: December 30, 2013, 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.

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 May 1, 2013:	The following activities support the recommendation that the baseline configurations for all systems be documented. • MD 12.5 is due to be released by September 30, 2013, and will provide updated NRC specific guidance for establishing configuration management requirements, processes and procedures. • CSO established the SWG which consists of participants from NRC offices who are stakeholders in the development of configuration baseline standards. The SWG is in the process of developing several configuration standards for existing and future technologies. As standards are developed and approved they are, where possible, converted into templates that can be used by the agency's configuration management scanning tool. The use of the tool provides the capability to automate the configuration monitoring of assets in the NRC production environment. • OIS currently has a configuration monitoring tool in place. Target Completion date: December 30, 2013, 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.

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 May 1, 2013:	OIS currently has a configuration monitoring tool in place. The activities associated with this recommendation are on schedule. Target 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.

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 May 1, 2013:	The activities associated with this recommendation are on schedule. Target 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.

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 May 1, 2013:	OIS currently has a configuration monitoring tool in place. The activities associated with this recommendation are on schedule. Target 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.