January 31, 2014

MEMORANDUM TO: Stephen D. Dingbaum
Assistant Inspector General for Audits

FROM: Thomas W. Rich, Director **/RA/**
Computer Security Office

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2011 (OIG-12-A-04)

In a memorandum to the Assistant Inspector General for Audits, dated May 1, 2013, (ML13098A178), and my office provided the Office of the Inspector General (OIG) with an updated status of the resolved recommendations to the subject report. This memorandum responds to the OIG's memorandum dated May 23, 2013, (ML 13143A210). In that memorandum, recommendations 1 through 6 were resolved, and the OIG requested an update on all recommendations.

This memorandum serves to provide the OIG a status update to the six recommendations discussed in its May 23, 2013, memorandum. It is also intended to inform you that the Computer Security Office (CSO), in coordination with the Office of Information Services (OIS), has completed the tasks needed to sufficiently address recommendation numbers 2 and 3. CSO requests these recommendations be considered closed.

Recommendation 1:

Develop and implement an organization-wide risk management strategy that is consistent with NIST SP 800-37 and NIST SP 800-39.

Response/Status Update:

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

Point of Contact: Kathy Lyons-Burke, CSO

CONTACT: Kathy Lyons-Burke, CSO
301-415-6595

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.

Response/Status Update:

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 comprise 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.

Point of Contact: Kathy Lyons-Burke, CSO, and David Offutt, OIS

Recommendation 3:

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

Response/Status Update:

- 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.

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2011

OIG-12-A-04

Status of Recommendations

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

Point of Contact: Kathy Lyons-Burke, CSO, and David Offutt, OIS

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.

Response/Status Update:

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

Point of Contact: Kathy Lyons-Burke, CSO, and David Offutt, OIS

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.

Response/Status Update:

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

Point of Contact: Kathy Lyons-Burke, CSO, and David Offutt, OIS

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.

Response/Status Update:

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

Point of Contact: Kathy Lyons-Burke, CSO, and David Offutt, OIS

cc: Chairman MacFarlane
Commissioner Svinicki
Commissioner Apostolakis
Commissioner Magwood
Commissioner Ostendorff
SECY

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.

Response/Status Update:

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

Point of Contact: Kathy Lyons-Burke, CSO, and David Offutt, OIS

cc: Chairman MacFarlane
Commissioner Svinicki
Commissioner Apostolakis
Commissioner Magwood
Commissioner Ostendorff
SECY

DISTRIBUTION: G20130417

RidsCSOMailCenter	RIDSOISResource	KOlive, OEDO
TRich, CSO	JFeibus, CSO	KLyons-Burke, CSO
ASage, CSO	DOffutt, CSO	

ADAMS Accession No.:ML131510334 (Pkg) ML14031A200 (Memo) *email concurrence

OFFICE	CSO	CSO	CSO	OIS*
NAME	KLyons-Burke for William Dabbs	JFeibus	TRich	DOffutt*
DATE	01/31/14	01/31/14	01/3/14	01/31/14

OFFICIAL RECORD COPY