May 1, 2013

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

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

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)

This responds to your memorandum dated December 29, 2011, requesting an updated status of the resolved recommendations on the subject report. Updates to the specific recommendations from our December 19, 2011, memorandum follows.

Recommendation 1:

Develop and implement an organization-wide risk management strategy that is consistent with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 and NIST SP 800-39.

Update:

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

Point of Contact: Ray Hardy, Computer Security Office (CSO)

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.

CONTACT: Ray Hardy, CSO/FCOT
301-415-5788

Update:

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 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

Point of Contact: 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.

Update:

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

Point of Contact: 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.

Update:

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

Point of Contact: 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.

Update:

The activities associated with this recommendation are on schedule.

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

Point of Contact: David Offutt, OIS

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.

Update:

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

Point of Contact: David Offutt, OIS

vulnerabilities, scan findings and security patch-related vulnerabilities, are remediated in a timely manner in accordance with the timeframes established by NRC.

Update:

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

Point of Contact: David Offutt, OIS

DISTRIBUTION: G20110877/EDATS: OEDO-2011-0799

RidsCsoMailCenter	RidsEdoMailCenter	RidsOigMailCenter
J. Flanagan, OIS	J. Arildsen, EDO	T. Rich, CSO
J. Feibus, CSO	R. Hardy, CSO	D. Offutt, OIS
G. Somerville, CSO		

ADAMS Accession No.: ML (Pkg.) 13098A089 ML13098A178 (Memo)

OFFICE	CSO	CSO/FCOT	OIS	CSO	CSO
NAME	GSomerville(see previous concurrence	RHardy (by TRich, see previous concurrence)	DOffutt (via email)	JFeibus (via email)	TRich (see previous concurrence
DATE	5 /1/2013	5/1/2013	5/1/ 2013	5/1/2013	5/1/2013

OFFICIAL RECORD COPY