

December 19, 2011

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

FROM: Darren B. Ash */RA/*  
Deputy Executive Director  
for Corporate Management  
Office of the Executive Director for Operations

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

This responds to the November 9, 2011, memorandum transmitting the subject audit report, which conveyed the findings and recommendations. With respect to your specific recommendations, I submit the following:

**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:**

Agree. NRC will develop and implement an organization-wide risk management strategy that is consistent with NIST SP 800-37 and NIST SP 800-39.

**Completion date:** December 30, 2013, pending availability of funds

**Point of Contact:** Paul Ricketts, 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.

**Response:**

Agree. NRC understands the importance of having clearly documented configuration management standards, and measurements to ensure that these standards are adequately adhered to. NRC will work to revise existing configuration management procedures with CSO and OIS working jointly to update our Project Management Methodology to include baseline configuration management procedures and appropriate performance measures along with

where possible, automated enterprise monitoring capabilities to ensure standard baseline configurations are implemented at the system component level.

**Estimated completion date:** December 30, 2013, pending availability of funds

**Point of Contact:** Paul Ricketts, 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:**

Agree. NRC understands the need to document the baseline configuration for information system components that are designated for configuration management, that have been formally reviewed and agreed on at a given point in time, and which can be changed only through approved change control procedures. Consequently, NRC will revise existing change control and associated configuration management procedures to include appropriate performance measures and where possible, automated enterprise monitoring capabilities to ensure baseline configurations are documented for all systems.

**Completion date:** December 30, 2013, pending availability of funds

**Point of Contact:** Paul Ricketts, 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:**

Agree. NRC understands that if an information system is inconsistent with approved configurations as defined by the organization's baseline configurations of system components, the System Security Plan, etc., or an organization's component inventory is inaccurate, the organization may be unaware of potential vulnerabilities and not take actions that would otherwise mitigate those vulnerabilities and protect the system from attacks. NRC will implement a configuration monitoring strategy to confirm that the existing configuration conforms to the current approved baseline configuration, that all items in the component inventory can be identified and are associated with the appropriate information system, and, if possible, whether there are any unapproved (i.e., not recorded in the component inventory) components and will revise existing change control and configuration management procedures to include appropriate performance measures and where possible, automated enterprise

monitoring capabilities to ensure software compliance assessments, including vulnerability assessments, are performed as required: (i) before a system component 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.

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

**Point of Contact:** Paul Ricketts, 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:**

Agree. NRC understands that an information system may have many components for which baseline configurations must be implemented and where practical, should ensure 100 percent of information system components are assessed for compliance and flaw remediation over time. NRC will implement a tool that adheres to the principals of the Security Protocol Automation Protocol developed by NIST for maintaining the security of enterprise systems to automatically verify the installation of patches, check system security configuration settings, and examine systems for signs of compromise and will revise existing configuration management procedures to include where possible, performance measures and automated enterprise monitoring capabilities to ensure all systems components are included in requisite software compliance assessments

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

**Point of Contact:** Paul Ricketts, CSO, and 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.

**Response:**

Agree. NRC understands that a systematic, accountable, and documented process for managing exposure to vulnerabilities through timely deployment of patches and mitigation of configuration-related and scan finding vulnerabilities is an essential security practice for proactive prevention of the exploitation of IT vulnerabilities that might exist within the agency. NRC will revisit the current management process and develop an approach for implementing a security patch and vulnerability remediation program and will revise existing configuration management procedures to include where possible, performance measures and automated

enterprise monitoring capabilities 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 best practices and timeframes established by NRC and within existing budgetary resources.

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

**Point of Contact:** Paul Ricketts, CSO, and David Offutt, OIS

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

enterprise monitoring capabilities 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 best practices and timeframes established by NRC and within existing budgetary resources.

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

**Point of Contact:** Paul Ricketts, CSO, and David Offutt, OIS

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

**DISTRIBUTION:** G20110794/EDATS: OEDO-2011-0732

RidsCsoMailCenter      RidsEdoMailCenter      RidsOigMailCenter      TBoyce, OIS      JSchaeffer, OIS  
JARildsen, EDO      RidsOgcMailCenter      RidsSecyMai Center      TRich, OIS      DOffutt, OIS

**ADAMS Accession No.:** ML11326A157 (Pkg.) ML11326A166 (Memo) \*via email

OFFICE	CSO/FCOT	OIS	CSO	DEDCM
NAME	PRicketts	TBoyce*	PHoward*	DAsh
DATE	12/15/2011	12/19/2011	12/19/2011	12/19/2011

**OFFICIAL RECORD COPY**