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

OFFICE OF THE
INSPECTOR GENERAL

October 25, 2017

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

FROM: Dr. Brett M. Baker ***/RA/***
Assistant Inspector General for Audits

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS (OIG-16-A-15)

REFERENCE: CHIEF INFORMATION OFFICER MEMORANDUM DATED SEPTEMBER 29, 2017

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated September 29, 2017. Based on this response, recommendations 1, 2, 5 and 7 are closed. Recommendations 4 and 6 remain resolved. Recommendation 3 was closed previously. Please provide an updated status of the resolved recommendations by April 30, 2018.

If you have questions or concerns, please call me at (301) 415-5915, or Beth Serepca, Team Leader at (301) 415-5911.

Attachment: As stated

cc: H. Rasouli, OEDO
R. Lewis, OEDO
J. Jolicoeur, OEDO
J. Bowen, OEDO
EDO_ACS Distribution

Audit Report

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendations

Recommendation 1:	Develop and document procedures for ensuring publicly accessible Web applications are assigned a system owner with responsibility for ensuring adequate security measures are in place for those applications.
Agency Response Dated September 29, 2017:	The Change Control Board (CCB) procedure has been revised to validate that a system owner has been named before a system change can be implemented. This process is mandatory for all system changes for new and existing systems. **Target Completion Date:** Completed The NRC requests that Recommendation 1 be closed.
OIG Analysis:	OIG reviewed the Change Control Board procedures and determined that the procedures state that a system owner will be named with responsibility for ensuring adequate security measures are in place for those applications. This recommendation is therefore considered closed.
Status:	Closed.

Audit Report

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendations

Recommendation 2:	Develop and document procedures for ensuring publicly accessible Web applications are incorporated into an approved system authorization boundary and for clearly identifying those applications in system authorization documentation.
Agency Response Dated September 29, 2017:	The system inventory has been updated to reflect ownership assignments, and system child/parent relationships. The Change Control Board (CCB) procedure has been revised to validate that a system has been incorporated into a system boundary before a system change can be implemented. This process is mandatory for all system changes for new and existing systems. **Target Completion Date:** Completed The NRC requests that Recommendation 2 be closed.
OIG Analysis:	OIG spoke with the point of contact and determined that NRC developed and documented the procedures for ensuring publicly accessible Web applications are incorporated into an approved system authorization boundary and for clearly identifying those applications in system authorization documentation. This recommendation is therefore considered closed.
Status:	Closed.

Audit Report

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendations

Recommendation 4:	Develop a plan and schedule to identify, review, and update all NRC cyber security standards that have not been updated in the past 12 months.
Agency Response Dated September 29, 2017:	The agency continues to move toward the use of public standards developed by the Center for Internet Security (CIS) and Defense Information System Agency (DISA). The review of existing standards has resulted in a number of standards being eliminated. The NRC is on track to meet the target completion date. **Target Completion Date:** Q2 FY 2018
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the implemented plan has a schedule to identify, review, and update all NRC cyber security standards that have not been updated in the past 12 months.
Status:	Resolved.

Audit Report

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendations

Recommendation 5:	Develop a plan and schedule for evaluating the vulnerabilities identified, determining the appropriate action to address the vulnerability (e.g., mitigation, deviation, risk acceptance), and implementing the remedial actions.
Agency Response Dated September 29, 2017:	The NRC has evaluated the vulnerabilities identified from the audit and created a program level plan of action and milestone (POA&M), POA&M ID 17-15, to address the vulnerabilities from the audit. Please refer to the POA&M details for the schedule and actions to be taken to address the vulnerabilities. Validation of remediated vulnerabilities will be conducted with an Open Web Application Security Project (OWASP) scanning tool. The OWASP scanning tool is planned for implementation by FY18 Q3. The NRC requests that Recommendation 5 be closed. **Target Completion Date:** Completed
OIG Analysis:	OIG's contractor reviewed the Plan of Actions and Milestones. OIG determined that NRC developed a plan and schedule for evaluating the vulnerabilities identified, determining the appropriate action to address the vulnerability (e.g., mitigation, deviation, risk acceptance), and implementing the remedial actions. This recommendation is therefore closed.
Status:	Closed.

Audit Report

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendations

Recommendation 6:	Complete the appropriate NRC RMF authorization activities for the NRC Webcast Portal.
Agency Response Dated September 29, 2017:	The NRC Webcast Portal has been authorized through March 31, 2019. ADM intends to award a new contract to a FED Ramp authorized service provider by the second quarter of 2019. The scope of the contract will include ensuring FISMA compliance. In addition, ADM has obligated funds to ensure that FISMA activities will be performed. **Revised Target Completion Date:** Q1 FY 2019
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when we receive verification that RMF authorization activities have been completed.
Status:	Resolved.

Audit Report

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendations

Recommendation 7:	Update CSO-PROS-2101 to include procedures for updating DNS entries and other resources allocated to new systems in addition to the inventory.
Agency Response Dated September 29, 2017:	The NRC continues to engage with system owners and system administrators. The Change Control Board (CCB) through the use of a change request form (CRQ), documents decommissioning efforts. The decommissioning process validates that all decommissioning steps are taken before the CRQ can be closed. This process is mandatory for all system changes for new and existing systems. The NRC is requesting that Recommendation 7 be closed.
OIG Analysis:	OIG spoke with the point of contact regarding the CQR and determined that it includes procedures for updating DNS entries and other resources allocated to new systems in addition to the inventory. This recommendation is therefore considered closed.
Status:	Closed.