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

OFFICE OF THE
INSPECTOR GENERAL

July 6, 2016

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

Stephen D. Dingbaum

FROM: Stephen D. Dingbaum
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: ACTING CHIEF INFORMATION OFFICER MEMORANDUM DATED JULY 1, 2016

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated July 1, 2016. Based on this response, recommendations 1-7 are resolved. Please provide an updated status of the resolved recommendations by April 3, 2017.

If you have questions or concerns, please call me at 415-5915, or Beth Serepca, Team Leader at 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 July 1, 2016: The NRC plans to update and implement the OIG recommended procedures by early Q2 FY 2017. The plan includes the verification of system owners for each publicly accessible Web application whose parent systems are currently registered in the NRC System Inventory; identification of additional applications for inclusion in the NRC System Inventory; revision of current process documents to require system owners to keep System Inventory data current and understand their roles and responsibilities for ensuring adequate security measures are in place for their applications; and communication of the revised process to all system owners.

Target Completion Date: Q2 FY

OIG Analysis: The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the implemented plan includes the verification of system owners for each publicly accessible Web application whose parent systems are currently registered in the NRC System Inventory.

Status: Resolved.

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 July 1, 2016: The NRC plans to update and implement the OIG recommended procedures no later than the end of Q2 FY 2017, as part of the effort described in our response to OIG recommendation 1. The plan includes that publicly accessible Web applications are incorporated into an approved system authorization boundary; revision of current process documents to ensure these applications are identifiable in system authorization documentation; and communication of the revised process to system owners.

Target Completion Date: Q2 FY 2017

OIG Analysis: The proposed actions meet the intent of the recommendation. OIG will close this recommendation when OIG receives verification 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.

Status: Resolved.

Audit Report

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

OIG-16-A-15

Status of Recommendations

Recommendation 3: Develop and document procedures for ensuring DHS is notified of any changes to the population of publicly accessible Web applications to be included in the Cyber Hygiene scans.

Agency Response Dated July 1, 2016: The NRC plans to develop and implement OIG recommended procedures no later than the end of Q2 FY 2017, as part of the effort described in our response to OIG Recommendation 1.

Target Completion Date: Q2 FY 2017

OIG Analysis: The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that the implemented plan includes notifying DHS of changes to the population so that those Web applications will be included in the Cyber Hygiene scans.

Status: Resolved.

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 July 1, 2016: The NRC will develop a plan and schedule to review and update all cyber security standards as needed.

Target Completion Date: Q1 FY 2017

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 July 1, 2016: The NRC will add all identified vulnerabilities to the appropriate Plan of Action & Milestone (POA&M) plans for ADAMS, BASS, ISMP, ITI, MOMCE, OCIMS, RICS, STAQS and VIDEO. The vulnerabilities will be managed and prioritized along with existing POA&M items.

Target Completion Date: Q4 FY 2016

OIG Analysis: The proposed actions meet the intent of the recommendation. OIG will close the recommendation when we receive the 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.

Status: Resolved.

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 July 1, 2016: The appropriate NRC RMF authorization activities for the NRC Webcast Portal are scheduled for completion in FY 2017.

Target Completion Date: Q1 FY 2017

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 July 1, 2016: The NRC will work with the appropriate NRC FISMA System Owners to integrate the procedures for decommissioning IT systems into existing Capital Planning and Investment Control governance processes to ensure all decommissioning instances are captured, DNS entries are updated, and system inventories are updated. When these efforts are completed, CSO-PROS-2101 will be rescinded.

Target Completion Date: Q3 FY 2017

OIG Analysis: The proposed actions meet the intent of the recommendation. OIG will close the recommendation when we receive verification that procedures for updating DNS entries and other resources allocated to new systems in addition to the inventory have been implemented.

Status: Resolved.