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

OFFICE OF THE
INSPECTOR GENERAL

July 12, 2017

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016 (OIG-17-A-03)

REFERENCE: CHIEF INFORMATION OFFICER MEMORANDUM DATED JUNE 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 June 29, 2017. Based on this response, recommendations 1 and 2 are closed and recommendations 3, 4, and 5 remain resolved. Please provide an updated status of the resolved recommendations by January 18, 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

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016

OIG-17-A-03

Status of Recommendations

Recommendation 1:	Develop a plan and schedule for ensuring all common controls are tested in accordance with NRC's continuous monitoring process.
Agency Response Dated June 29, 2017:	The assessment has been completed. The Information Security Planning and Oversight Branch needs to review the results and confirm the findings. The Authorizing Official will be briefed on the results by July 31 for his approval. **Target completion date:** July 31, 2017
OIG Analysis:	The recommendation requested that a plan and a schedule be developed to test all common controls. From our FISMA evaluation work that is ongoing at this time, OIG determined that there is a plan and a schedule. The agency is now in the testing phase. This recommendation is therefore considered closed.
Status:	Closed.

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016

OIG-17-A-03

Status of Recommendations

Recommendation 2:	Develop a plan and schedule for developing a comprehensive inventory of all NRC systems.
Agency Response Dated June 29, 2017:	This planning effort has been completed. Through coordination of multiple branches, the NRC developed a plan for improvement. The execution of this plan has further improved the data in the inventory of NRC Systems and Services. The plan included identification of contractor systems, modifications to the method of handling classified systems and web-accessible systems. Initial identification of contractor and other systems/services has been made, the inventory has been updated and the update process will continue. The list of contractor systems has been forwarded to OIG for the 2017 FISMA audit activity. **Target completion date:** Completed
OIG Analysis:	OIG has received the inventory for its FISMA evaluation, and through the ongoing FISMA work, determined that the agency developed a plan and schedule as well as an inventory of NRC Systems. This recommendation is therefore considered closed.
Status:	Closed.

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016

OIG-17-A-03

Status of Recommendations

Recommendation 3:	Develop supporting processes, procedures, and guidance for ensuring the NRC systems inventory is maintained.
Agency Response Dated June 29, 2017:	The completion date for this activity has changed to reflect integration and coordination with owners of related Office of Management and Budget CyberStat actions that eliminates redundant work activities and implements a common continuous monitoring and diagnostics approach. Revised target completion date: December 29, 2017
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close this recommendation when OIG receives evidence showing NRC has developed supporting processes, procedures, and guidance for ensuring the NRC systems inventory is maintained.
Status:	Resolved.

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016

OIG-17-A-03

Status of Recommendations

Recommendation 4:	Based on the updated inventory of contractor systems, identify those that are not complaint with ISD-PROS-2030, *NRC Risk Management Framework*, and complete appropriate authorization activities for those systems.
Agency Response Dated June 29, 2017:	OCIO has identified systems not in compliance with the NRC Risk Management Framework, and continues to coordinate with stakeholders to obtain or maintain appropriate system authorizations. The NRC will continue to assemble required evidence of risk management activities in support of system authorizations. The ATU schedule briefed to the CIO has extended out through April 2018 due to delays in acquiring contractor support. **Revised target completion date:** June 29, 2018
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close this recommendation when OIG receives evidence showing NRC has identified those contractor systems that are not compliant with ISD-PROS-2030, *NRC Risk Management Framework*, and completes appropriate authorization activities for these systems.
Status:	Resolved.

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016

OIG-17-A-03

Status of Recommendations

Recommendation 5:	Develop procedures for ensuring the annual IT risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.
Agency Response Dated June 29, 2017:	OCIO expects to update relevant processes to ensure that annual IT security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements. Additionally, risk management activities as outlined in ISD-PROS-2030 (and interactions with internal and external system owners) are planned to be tracked in one central location to facilitate visibility, management, and timely compliance. **Target completion date:** December 29, 2017
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when OIG receives evidence that NRC has developed procedures for ensuring the annual IT risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.
Status:	Resolved.