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

OFFICE OF THE
INSPECTOR GENERAL

December 28, 2016

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 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 DECEMBER 7, 2016

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated December 7, 2016. Based on this response, recommendations 1, 2, 3, 4, and 5 are resolved. Please provide an updated status of the resolved recommendations by June 30, 2017.

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: D. Nelson, OCIO
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 December 7, 2016:	Agree. The Office of the Chief Information Officer (OCIO) will develop a plan and schedule to complete testing of common controls is accordance with NRC's continuous monitoring process. Target date for completion: July 31, 2017
OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that NRC provides evidence demonstrating that OCIO has developed a plan and schedule for ensuring all common controls are tested in accordance with NRC's continuous monitoring process.
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 2:	Develop a plan and schedule for developing a comprehensive inventory of all NRC systems.
Agency Response Dated December 7, 2016:	Agree. The NRC will develop a plan and schedule for creating a comprehensive inventory of all NRC systems. Target date for completion: June 30, 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 a plan and schedule for developing a comprehensive inventory for all NRC 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 3:	Develop supporting processes, procedures, and guidance for ensuring the NRC systems inventory is maintained.
Agency Response Dated December 7, 2016:	Agree. The NRC will review and update all internal processes, policies, and procedures to ensure that proper authorities, roles, and responsibilities regarding the maintenance of the NRC systems inventory are clearly documented. The inventory procedures will include the following: a. All required system documentation and authoritative repositories b. Identification of a single technical point of contact for each system c. References for review of updates to system documentation d. References for random validation of system information e. A process for documenting systems containing classified data f. Documentation of the process for recording systems not currently recorded in inventory that are identified through random scanning of the production environment Target date for completion: March 31, 2017
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close this recommendation when OIG receives evidence showing NRC has Develop 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 December 7, 2016:	Agree. Based upon the updated inventory of systems, OCIO will identify those that are not compliant with the NRC Risk Management Framework and complete appropriate authorization activities for those systems. OCIO will engage support staff and other stakeholders, such as system owners, share service providers, cloud service providers, to ensure that appropriate evidence of risk management activities is available to support authorization activities. Target date for completion: 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 identified those contractor systems that are not compliant with ISD-PROS-2030, *NRC Risk Management Framework*, and completes appropriate activities
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 December 7, 2016:	Agree. OCIO will develop procedures for ensuring the annual IT security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements. OCIO will develop a plant to ensure that all systems owned or operated by other agencies that NRC relies upon go through appropriate risk management activities as outline in ISD-PROS-2030, and will ensure interactions with internal and external system owners are managed and tracked. Target date for completion: 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.