January 25, 2018

MEMORANDUM TO: Dr. Brett M. Baker
Assistant Inspector General for Audits
Office of the Inspector General

FROM: David J. Nelson **/RA/**
Chief Information Officer
Office of the Chief Information Officer

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

As requested in your December 28, 2016, memorandum, enclosed please find the updated status to recommendations 3, 4, and 5 contained in the subject report.

Recommendations 1 and 2 were previously closed.

Enclosure:
Status of Recommendations 3-5

cc: Steven Zane, OIG

CONTACT: Cathy E. Smith, OCIO/GEMSD
(301) 415-5648

Response to OIG's Independent Evaluations of the NRC's Implementation of The Federal Information Security Modernization Act of 2014 For Fiscal Year 2016 (OIG-17-A-03)
DATE: January 25, 2018

DISTRIBUTION: OEDO-17-00459 (OIG-17-A-03)
RidsOigMailCenter Resource
RidsEdoMailCenter Resource
RidsOCIO Resource

ADAMS Accession No: Pkg.: ML17194A796; Memo: ML18024A177 *via email

OFFICE:	OCIO/GEMS/ISPOB	OCIO/GEMSD/EAB	OCIO/GEMSD/EAB	OCIO/GEMSD/PIMB
NAME:	BC: ASullivan*	JBeatty*	BC: ELeong* (NBuggs* for)	CSmith*
DATE:	01/22/2018	01/22/2018	01/24/2018	01/24/2018
OFFICE	OCIO/GEMSD/PIMB	OCIO/GEMSD	OCIO/GEMSD	OCIO
NAME	BC: MYimam*	DD: JFeibus*	D: JMoses*	D: DNelson
DATE	01/24/2018	01/23/2018	01/24/2018	01/25/2018

OFFICIAL RECORD COPY

INDEPENDENT EVALUATIONS OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA) 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 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 Completion Date:** March 31, 2017
Agency Response Dated June 21, 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. **Target Completion Date:** December 29, 2017
Agency Response Dated January 19, 2018:	The completion date for this activity has changed to align with a common continuous monitoring and diagnostics approach. **Revised Target Completion Date:** December 31, 2018 **Point of Contact:** John Beatty, 301-415- 5774

Recommendation 4:	Based on the updated inventory of contractor systems, identify those that are not compliant 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, shared service providers, cloud service providers, to ensure that appropriate evidence of risk management activities is available to support authorization activities. **Target Completion Date:** December 29, 2017
Agency Response Dated June 15, 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
Agency Response Dated January 19, 2018:	The NRC is on track to meet the completion date. All but 2 of 30 contractor systems are authorized. The 2 remaining systems will have authorizations before the end of June 2018. **Target Completion Date:** June 29, 2018 **Point of Contact:** Aldo Eskandary, 301-415-0088 Allen Sullivan, 240-415-8950

Recommendation 5:	Develop procedures for ensuring that 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.
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 plan to ensure that all systems (NRC and contractor owned) go through appropriate risk management activities as outlined in ISD- PROS-2030, and will ensure interactions with internal and external system owners are managed. **Target Completion Date:** December 29, 2017
Agency Response Dated June 15, 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
Agency Response Dated January 19, 2018:	The NRC has completed this recommendation. The tracking of risk management activities in one central place has been completed. The FY17 CyberScope report indicated 27 of 30 systems are authorized and that 17 of the 27 are in ongoing authorization. **Target Completion Date:** Completed **Point of Contact:** Alan Sage, 301-415-7060