



OFFICE OF THE
INSPECTOR GENERAL

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

February 15, 2018

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
JANUARY 25, 2018, AND SUBSEQUENT EMAIL
CORRESPONDENCE

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated January 25, 2018, and subsequent email correspondence. Based on this response, recommendation 5 is closed. Recommendations 3 and 4 remain resolved. Recommendations 1 and 2 were closed previously. Please provide an updated status of the resolved recommendations by July 2, 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 3: Develop supporting processes, procedures, and guidance for ensuring the NRC systems inventory is maintained.

Agency Response Dated
January 25, 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

OIG Analysis: The proposed actions as initially identified in the agency's response dated December 7, 2016, meet the intent of the recommendation. OIG understands the need to revise the completion dated and 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 compliant with ISD-PROS-2030, *NRC Risk Management Framework*, and complete appropriate authorization activities for those systems.

Agency Response Dated
January 25, 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

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.

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
February 8, 2018:

The NRC has completed this recommendation. In FY17, OCIO developed the External Information Technology Service Authorization Process and Checklist as well as the Authorization Plan for External Information Technology Services. The implementation of these documents, together with the existing Information Security Continuous Monitoring Process and System Cybersecurity Assessment Process, as of February 8, 2018, have resulted in the authorization 26 of 27 external systems (contractor or Government Shared Service Provider) in use by the NRC.

Target Completion Date: Completed

OIG Analysis:

OIG spoke with the point of contact for this recommendation. OCIO recognized that the new procedures were not needed. Instead, the OCIO used existing procedures to ensure that the annual security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements. Further, OCIO developed a plan to ensure tracking of all risk management activities in a central place. OCIO provided evidence of the plans to OIG. OIG determined that OCIO is now 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. This recommendation is therefore considered 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 5 (cont.):

Status: Closed.