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

OFFICE OF THE
INSPECTOR GENERAL

August 15, 2019

MEMORANDUM TO: Margaret M. Doane
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018 (OIG-19-A-08)

REFERENCE: DEPUTY EXECUTIVE DIRECTOR FOR MATERIALS, WASTE, RESEARCH, STATE, TRIBAL, COMPLIANCE, ADMINISTRATION, AND HUMAN CAPITAL PROGRAMS MEMORANDUM DATED MAY 1, 2019

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated May 1, 2019. Based on this response, recommendations 1 through 6 are open and resolved. Please provide an updated status of the open and resolved recommendations by January 31, 2020.

If you have questions or concerns, please call me at (301) 415-5915, or Eric Rivera, Team Leader, at (301) 415-7032.

Attachment: As stated

cc: C. Haney, OEDO
D. Jackson, OEDO
J. Jolicoeur, OEDO
S. Miotla, OEDO
RidsEdoMailCenter Resource
OIG Liaison Resource
EDO_ACS Distribution

Audit Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018

OIG-19-A-08

Status of Recommendations

Recommendation 1:	Develop and implement a process to remove all non-standard software that has not been approved by an authorized agency official.
Agency Response Dated May 01, 2019:	The U.S. Nuclear Regulatory Commission (NRC) will develop and implement a process to remove all nonstandard software that has not been approved by an authorized agency official. Target Completion Date: March 31, 2020
OIG Analysis:	The actions proposed by the agency meet the intent of the recommendation. OIG will close this recommendation upon receipt of documentation showing a process to remove all non-standard software that has not been approved by an authorized agency official has been developed and implemented.
Status:	Open: Resolved.

Audit Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018

OIG-19-A-08

Status of Recommendations

Recommendation 2:	Implement a process to manage non-standard software to ensure the software is properly approved and inspected for security weaknesses before the software is installed on NRC's network.
Agency Response Dated May 01, 2019:	The NRC will implement a process to manage nonstandard software to ensure the software is properly approved and inspected for security weaknesses before the software is installed on the NRC's network. The agency will review and update the current Office of the Chief Information Officer (OCIO) process for Information Technology (IT) Business Need Requests to meet the requirements outlined in Recommendation 2. In addition, the new End User Computing contract specifies that all software must be approved and have a service ticket before software may be installed. **Target Completion Date:** December 31, 2019
OIG Analysis:	The actions proposed by the agency meet the intent of the recommendation. OIG will close this recommendation upon receipt of documentation showing the staff implemented a process to manage non-standard software to ensure the software is properly approved and inspected for security weaknesses before the software is installed on NRC's network.
Status:	Open: Resolved.

Audit Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018

OIG-19-A-08

Status of Recommendations

Recommendation 3:	Monitor the approved installed software on NRC's network to determine whether it is still in use, periodically inspect the software for known vulnerabilities, and mitigate any vulnerabilities found.
Agency Response Dated May 01, 2019:	The NRC will monitor the approved installed software on the agency's network to determine whether it is still in use, periodically inspect the software for known vulnerabilities, and mitigate any vulnerabilities found. **Target Completion Date:** December 31, 2019
OIG Analysis:	The actions proposed by the agency meet the intent of the recommendation. OIG will close this recommendation upon receipt of documentation showing NRC monitored approved installed software on NRC's network, periodically inspected the software for known vulnerabilities, and mitigated any vulnerabilities found.
Status:	Open: Resolved.

Audit Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018

OIG-19-A-08

Status of Recommendations

Recommendation 4:	Develop and establish processes and procedures to govern the installation of non-standard software, including processes and procedures on determining impact to agency operations or cybersecurity.
Agency Response Dated May 01, 2019:	The NRC will develop and establish processes and procedures to govern the installation of nonstandard software, including processes and procedures for determining the impact to agency operations or cybersecurity. The agency will review and update the current OCIO process for IT Business Need Requests to meet the requirements outlined in Recommendation 4. The new End User Computing contract specifies that all software must be approved and have a service ticket before software may be installed. **Target Completion Date:** December 31, 2019
OIG Analysis:	The actions proposed by the agency meet the intent of the recommendation. OIG will close this recommendation upon receipt of documentation showing NRC developed and established processes and procedures to govern the installation of nonstandard software, including processes and procedures for determining the impact to agency operations or cybersecurity.
Status:	Open: Resolved.

Audit Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018

OIG-19-A-08

Status of Recommendations

Recommendation 5:	Implement a process to remove unsupported software from NRC networks.
Agency Response Dated May 01, 2019:	The NRC will develop and implement a process to remove unsupported software from the agency's network environment. **Target Completion Date:** March 31, 2020
OIG Analysis:	The actions proposed by the agency meet the intent of the recommendation. OIG will close this recommendation upon receipt of documentation showing NRC developed and implemented a process to remove unsupported software from the agency's network environment.
Status:	Open: Resolved.

Audit Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018

OIG-19-A-08

Status of Recommendations

Recommendation 6:	Implement a process to mitigate known high-risk vulnerabilities.
Agency Response Dated May 01, 2019:	The NRC will implement a process to mitigate known high-risk vulnerabilities for application software that resides on NRC networks. **Target Completion Date:** December 31, 2019
OIG Analysis:	The actions proposed by the agency meet the intent of the recommendation. OIG will close this recommendation upon receipt of documentation showing NRC implemented a process to mitigate known high-risk vulnerabilities for application software that resides on NRC networks.
Status:	Open: Resolved.