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

OFFICE OF THE
INSPECTOR GENERAL

February 11, 2021

MEMORANDUM TO: Margaret M. Doane
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019 (OIG-20-A-06)

REFERENCE: CHIEF INFORMATION OFFICER; OFFICE OF THE CHIEF INFORMATION OFFICER MEMORANDUM DATED JANUARY 14, 2021

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated January 14, 2021. Based on this response, recommendation 3 is closed and recommendations 1, 2, and 4–7 are in open and resolved status. Please provide an update on the status of these resolved recommendations by July 15, 2021.

If you have questions or concerns, please call me at (301) 415-5915, or Terri Cooper, Team Leader, at (301) 415-5965.

Attachment: As stated

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

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 1:	Fully define NRC's ISA across the enterprise and business processes and system levels.
Agency Response Dated January 14, 2021:	Working on Information Security Architecture (ISA) using the National Institute of Standards and Technology Cybersecurity Framework. Currently on schedule. Target Completion Date: Q2 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC fully defines the ISA across enterprise and business processes and system levels.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 2a:	Use the fully defined ISA to assess enterprise, business process, and information system level risks.
Agency Response Dated January 14, 2021:	Preliminary planning is complete, waiting for the completion of the ISA to assess enterprise, business process, and information system level risks. Target Completion Date: Q3 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC uses the fully defined ISA to assess enterprise, business process, and information system level risks.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 2b:	Use the fully defined ISA to update the list of high value assets by considering risks from the supporting business functions and mission impacts.
Agency Response Dated January 14, 2021:	Waiting for completion of ISA. Currently on schedule. Target Completion Date: Q2 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC uses the fully defined ISA to update the list of high value assets by considering risks from the supporting business functions and mission impacts.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 2c:	Use the fully defined ISA to formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.
Agency Response Dated January 14, 2021:	Waiting for completion of ISA. Currently on schedule. Target Completion Date: Q3 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC uses the fully defined ISA to formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 2d:	Use the fully defined ISA to conduct an organization-wide security and privacy risk assessment.
Agency Response Dated January 14, 2021:	Waiting for completion of ISA. Currently on schedule. Target Completion Date: Q4 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC uses the fully defined ISA to conduct an organization-wide security and privacy risk assessment.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 2e:	Use the fully defined ISA to conduct a supply chain risk assessment.
Agency Response Dated January 14, 2021:	Waiting for completion of ISA. Currently on schedule. Target Completion Date: Q4 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC uses the fully defined ISA to conduct a supply chain risk assessment.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 2f:	Use the fully defined ISA to identify and update NRC risk management policies, procedures, and strategy.
Agency Response Dated January 14, 2021:	Waiting for completion of ISA. Currently on schedule. Target Completion Date: Q1 FY 2022
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC uses the fully defined ISA to identify and update NRC risk management policies, procedures, and strategy.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 3:	Identify and implement a software whitelisting tool to detect authorized software and block the risk of unauthorized software on its network.
Agency Response Dated January 14, 2021:	The NRC identified and implemented a solution to detect authorized software and block unauthorized software on the network. The Office of the Chief Information Officer (OCIO) has deployed Palo Alto Cortex XDR software to block attempts to run unauthorized software that is not included in the NRC Technical Reference Model. The activity was announced to staff on September 08, 2020 and blocking unauthorized software on agency workstations began on September 17, 2020. Target Completion Date: Complete
OIG Analysis:	The OIG reviewed and verified that the NRC identified and implemented a tool to detect authorized software and block the risk of unauthorized software on its network. Therefore, recommendation 3 is now closed.
Status:	Closed.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 4:	Perform an assessment of role-based privacy training gaps.
Agency Response Dated January 14, 2021:	Assessment of Training gaps has been tasked to an OCIO contractor with the project set to commence the week of January 10, 2020. Currently on schedule for a completion date of March 31, 2021. Target Completion Date: Q2 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC performs an assessment of role-based privacy training gaps.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 5:	Identify individuals having specialized role-based responsibilities for PII or activities involving PII and develop role-based privacy training for them.
Agency Response Dated January 14, 2021:	OCIO has identified the Information System Security Officer and System Administrator as having personally identifiable information (PII) responsibilities. These roles are being incorporated into the agency's privacy training program. Other roles may be identified once the agency's assessment of training gaps is completed in Q2 FY 2021, delaying the closing of this recommendation. Target Completion Date: Q2 FY 2022
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC completes the training gap assessment and identifies individuals having specialized role-based responsibilities for PII or activities involving PII and develop role-based privacy training for them.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 6:	Based on NRC's supply chain risk assessment results, complete updates to the NRC's contingency planning policies and procedures to address supply chain risk training for them.
Agency Response Dated January 14, 2021:	Waiting for completion of Supply Chain Risk Assessment. Currently on schedule. Target Completion Date: Q1 FY 2022
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC uses the results from the supply chain risk assessment to complete updates to the NRC's contingency planning policies and procedures to address supply chain risk.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019

OIG-20-A-06

Status of Recommendations

Recommendation 7:	Continue efforts to conduct agency and system level business impact assessments to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.
Agency Response Dated January 14, 2021:	Waiting for completion of ISA. Currently on schedule. Target Completion Date: Q1 FY 2022
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC continues efforts to conduct agency and system level business impact assessments to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.
Status:	Open: Resolved.