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

OFFICE OF THE
INSPECTOR GENERAL

September 21, 2021

MEMORANDUM TO: Margaret M. Doane
Executive Director for Operations

FROM: Eric Rivera ***/RA/***
Acting 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: DEPUTY EXECUTIVE DIRECTOR FOR MATERIALS, WASTE, RESEARCH, STATE, TRIBAL, COMPLIANCE, ADMINISTRATION, AND HUMAN CAPITAL PROGRAMS; OFFICE OF THE EXECUTIVE DIRECTOR FOR OPERATIONS MEMORANDUM DATED JULY 15, 2021

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated July 15, 2021. Based on this response, recommendations one, and 2.b are closed; and 2.a, 2.c-f, and four – seven are in open and resolved status. Recommendation three was closed previously. Please provide an update on the status of the open and resolved recommendations by **January 14, 2022.**

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. Mroz, OEDO
J. Jolicoeur, OEDO
S. Miotla, 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 July 15, 2021:	Information Security Architecture (ISA) signed by the Chief Information Security Officer (CISO) and Deputy Chief Information Officer (CIO) on July 2, 2021. Target Completion Date: Complete
OIG Analysis:	The OIG reviewed the ISA signed by the CISO and Deputy CIO and noted that the OCIO had defined NRC's ISA fully across the enterprise and business processes and system levels. This recommendation is therefore 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 2.a:	Use the fully defined ISA to assess enterprise, business process, and information system level risks.
Agency Response Dated July 15, 2021:	After analyzing the finalized ISA and looking at the impacts the ISA had on this task, we will need an extension from FY21 Q4 to FY22 Q2. Currently on schedule for completion FY22 Q2. Developing a plan to modify the agency's processes that were impacted by the development of the ISA. Piloting a new risk model that contains 5 levels of risk (Very High, High, Moderate, Low, Very Low) instead of 3 levels of risk (High, Moderate, Low). Not only will this help the agency prioritize deficiencies in a more efficient manner, but it will allow the agency to consistently measure risk across its cybersecurity program. Target Completion Date: FY22 Q2
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. Therefore, this recommendation remains open and resolved.
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 2.b:	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 July 15, 2021:	The list of NRC High Valued Assets (HVAs) have been aligned to the finalized ISA. This determination was made based on the system's involvement in supporting NRC's primary mission essential functions and mission essential functions. Target Completion Date: Complete
OIG Analysis:	The OIG reviewed the list of HVAs and verified that the OCIO had aligned the HVAs to the finalized ISA. Therefore, this recommendation is 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 2.c:	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 July 15, 2021:	Currently on schedule. The finalized ISA and the 5-level risk model pilot are being analyzed so a plan can be developed to address this recommendation. Target Completion Date: FY22 Q1
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. Therefore, this recommendation remains open and resolved.
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 2.d:	Use the fully defined ISA to conduct an organization-wide security and privacy risk assessment.
Agency Response Dated July 15, 2021:	Currently on schedule. NRC is developing a 3-year cycle to assess the entire ISA. The first-year assessment will focus on the identify function, recent health checks that were performed against NRC's infrastructure, system Plan of Action and Milestone reports, and deficiencies associated with NRC's most critical cloud providers. Target Completion Date: FY22 Q1
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. Therefore, this recommendation remains open and resolved.
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 2.e:	Use the fully defined ISA to conduct a supply chain risk assessment.
Agency Response Dated July 15, 2021:	Supply chain risk analysis solution is currently being procured. Procurement is expected by the end of the current fiscal year. Since the task is on hold until the procurement is completed, we will need to extend this recommendation's completion date from FY22 Q1 to FY22 Q4. Currently on schedule for completion FY22 Q4. Target Completion Date: FY22 Q4
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the agency uses the fully defined ISA to conduct a supply chain risk assessment. Therefore, this recommendation remains open and resolved.
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 2.f:	Use the fully defined ISA to identify and update NRC risk management policies, procedures, and strategy.
Agency Response Dated July 15, 2021:	After analyzing the finalized ISA and looking at the impact recommendation 2a and 2c have on this task, we will need an extension from FY22 Q1 to FY22 Q3. Currently on schedule for completion FY22 Q3. Currently developing a plan and reviewing the finalized ISA, recommendation 2a, and recommendation 2c. Target Completion Date: FY22 Q3
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when the NRC uses the fully defined ISA to identify and update NRC risk management policies, procedures, and strategy. Therefore, this recommendation remains open and resolved.
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 4:	Perform an assessment of role-based privacy training gaps.
Agency Response Dated July 15, 2021:	The assessment of the role-based privacy training gaps has been completed. Target Completion Date: Complete
OIG Analysis:	The agency could not provide a written assessment of the role-based privacy training gaps and stated that they had updated role-based privacy training based on staff knowledge. The OIG will close this recommendation when the agency provides an assessment of role-based privacy training gaps. Therefore, this recommendation remains open and resolved.
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 July 15, 2021:	Currently on schedule. 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 are completed in Q2 FY 2021, delaying the closing of this recommendation. Target Completion Date: FY22 Q2
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC determines if any other roles were identified during the agency's assessment of training gaps. Therefore, this recommendation remains open and resolved.
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 July 15, 2021:	This task is dependent on recommendation 2e being completed. Given the extension requested for 2e, this task needs extended from FY22 Q1 to FY23 Q1. Target Completion Date: FY23 Q1
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 NRC's contingency planning policies and procedures to address supply chain risk. Therefore, this recommendation remains open and resolved.
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 July 15, 2021:	Currently on schedule. OCIO will evaluate the finalized ISA and the agency's contingency planning requirements to determine the impact and related updates to policies and procedures that need to be performed. Target Completion Date: FY22 Q1
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. Therefore, this recommendation remains open and resolved.
Status:	Open: Resolved.