August 9, 2022

MEMORANDUM TO: Daniel H. Dorman
Executive Director for Operations

FROM: Eric Rivera */RA/*
Acting 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 2019 (OIG-20-A-06)

REFERENCE: CHIEF INFORMATION OFFICER, OFFICE OF THE CHIEF INFORMATION OFFICER, MEMORANDUM DATED JULY 15, 2022

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, 2022. Based on this response, 2.a, 2.c-f, and 4 – 7 are in open and resolved status. Recommendations 1, 2.b, and 3 were closed previously. Please provide an update on the status of the open and resolved recommendations by **January 15, 2023.**

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: M. Bailey, OEDO
E. Stahl, OEDO
J. Jolicoeur, 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 2a:	Use the fully defined ISA to assess enterprise, business process, and information system level risks.
Agency Response Dated July 15, 2022:	After analyzing the finalized information system architecture (ISA) and assessing the impacts related to this task, the U.S. Nuclear Regulatory Commission (NRC) plans to complete this task by the fourth quarter (Q) of fiscal year (FY) 2022. To address this recommendation, the NRC is developing a plan to modify the Agency's processes that were impacted by the development of the ISA and is piloting a new risk model that contains five levels of risk (Very High, High, Moderate, Low, Very Low) instead of three 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:** FY 2022, Q4 **Point of Contact:** Bill Dabbs, OCIO/GEMS/CSB 301-415-0524
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 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 July 15, 2022:	The finalized ISA and the five-level risk model pilot will be analyzed so a plan can be developed to address this recommendation. **Target Completion Date:** FY 2023, Q2 **Points of Contact:** Garo Nalabandian, OCIO/CISO 301-415-8421
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 2d:	Use the fully defined ISA to conduct an organization-wide security and privacy risk assessment.
Agency Response Dated July 15, 2022:	The 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 performed against the NRC's infrastructure, system plan of action and milestone reports, and deficiencies associated with the NRC's most critical Cloud providers. **Target Completion Date:** FY 2022, Q4 **Point of Contact:** Bill Dabbs, OCIO/GEMS/CSB 301-415-0524 Sally Hardy, OCIO/GEMSD/CSB 301-415-5607
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 2e: Use the fully defined ISA to conduct a supply chain risk assessment.

Agency Response Dated July 15, 2022: A supply chain risk analysis solution has been procured. The NRC is currently determining its processes to use the tool to assess supply chain risk. This task is currently on schedule for completion in FY 2023, Q2.

Target Completion Date: FY 2023, Q2

Points of Contact: Garo Nalabandian, OCIO/CISO
(301) 415-8421

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 2f:	Use the fully defined ISA to identify and update NRC risk management policies, procedures, and strategy.
Agency Response Dated July 15, 2022:	After analyzing the finalized ISA and assessing the impacts of recommendation 2a and 2c on this task, the NRC plans to complete the task in FY 2023, Q3. **Target Completion Date:** FY 2023, Q3 **Points of Contact:** Bill Bauer, OCIO/GEMSD/CSB 301-415-8513
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, 2022:	The NRC is evaluating current resources to determine support for developing a written assessment of gaps in role-based privacy training. **Target Completion Date:** FY 2022, Q4 **Point of Contact:** Bill Bauer, OCIO/GEMS/CSB 301-415-8513 Sally Hardy, OCIO/GEMSD/CSB 301-415-5607
OIG Analysis:	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, 2022:	This task is currently on schedule. The NRC has identified the Information System Security Officer and System Administrator as having responsibilities for personally identifiable information (PII). These roles are being incorporated into the Agency's privacy training program. **Target Completion Date:** FY 2022, Q4 **Point of Contact:** Bill Bauer, OCIO/GEMS/CSB 301-415-8513 Sally Hardy, OCIO/GEMSD/CSB 301-415-5607
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, 2022:	This task is dependent on the completion of recommendation 2e. Given the extension requested for recommendation 2e, this task needs to be extended from FY 2022, Q1, to FY 2023, Q2. **Target Completion Date:** FY 2023, Q2 **Point of Contact:** Garo Nalabandian, OCIO/CISO 301-415-8421
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, 2022:	This task is currently on schedule. The NRC will evaluate the finalized ISA and the Agency's contingency planning requirements to determine the impact and related necessary updates to policies and procedures. **Target Completion Date:** FY 2023, Q3 **Point of Contact:** Garo Nalabandian, OCIO/CISO 301-415-8421 Debra Reyes, OCIO/ITSDOD/DCTSB 301-287-0681
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.