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

OFFICE OF THE
INSPECTOR GENERAL

July 30, 2020

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 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, 2020

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, 2020. Based on this response, recommendations 1 – 7 are in open and resolved status. Please provide an update on the status of these resolved recommendations by January 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
J. Quichocho, 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, 2020:	The U.S. Nuclear Regulatory Commission (NRC) will fully define the Information Security Architecture (ISA) across the enterprise and business processes and system levels. Target Completion Date: Q2 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when 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 July 15, 2020:	The NRC will use the fully defined 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. OIG will close the recommendation when 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 July 15, 2020:	The NRC will use the fully defined ISA to update the list of high value assets by considering risks from the supporting business functions and mission impacts. Target Completion Date: Q2 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when 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.
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, 2020:	The NRC will 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. Target Completion Date: Q3 FY 2021

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 (cont'd):

OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when 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.
Recommendation 2d:	Use the fully defined ISA to conduct an organization-wide security and privacy risk assessment.
Agency Response Dated July 15, 2020:	The NRC will use the fully defined ISA to conduct an organization-wide security and privacy risk assessment. Target Completion Date: Q4 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when 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 July 15, 2020:	The NRC will use the fully defined ISA to conduct a supply chain risk assessment. Target Completion Date: Q4 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when NRC uses the fully defined ISA to conduct a supply chain risk assessment.
Status:	Open: Resolved.
Recommendation 2f:	Use the fully defined ISA to identify and update NRC risk management policies, procedures, and strategy.
Agency Response Dated July 15, 2020:	The NRC will use the fully defined ISA to identify and update NRC risk management policies, procedures, and strategy. Target Completion Date: Q1 FY 2022
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when 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 July 15, 2020:	The NRC will identify and implement a tool to detect authorized software and block the risk of unauthorized software on its network. Target Completion Date: Q4 FY 2020
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when NRC identifies and implements a tool to detect authorized software and block the risk of unauthorized software on its network.
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, 2020:	The NRC will perform an assessment of role-based privacy training gaps. Target Completion Date: Q2 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when 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 July 15, 2020:	The NRC will Identify individuals having specialized role-based responsibilities for PII or activities involving PII and develop role-based privacy training for them. Target Completion Date: Q3 FY 2021
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when NRC 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 July 15, 2020:	The NRC will use 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. Target Completion Date: Q1 FY 2022
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when 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.
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, 2020:	The NRC will 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. Target Completion Date: Q1 FY 2022
OIG Analysis:	The proposed actions meet the intent of the recommendation. OIG will close the recommendation when 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.